NWA5120 Series

802.11 a/b/g/n Unified Access Point

Version 2.25
Edition 1, 01/2013

User's Guide

Default Login Details	
LAN IP Address	http://192.168.1.2
User Name	admin
Password	1234

Copyright © 2013 ZyXEL Communications Corporation

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a User's Guide for a series of products. Not all products support all firmware features. Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the NWA and access the Web Configurator.

Contents Overview

User's Guide 11

Introduction 13
The Web Configurator 19

Technical Reference 31

Dashboard 33
Monitor 39
LAN Setting 51
Wireless 53
User 65
AP Profile 73
MON Profile 91
Certificates 95
System 113
Log and Report 139
File Manager 151
Diagnostics 163
Reboot 165
Shutdown 167
Troubleshooting 169

Table of Contents

Contents Overview **3**

Table of Contents **5**

Part I: User's Guide **11**

Chapter 1
Introduction **13**

1.1 Overview 13
1.1.1 MBSSID 14
1.1.2 Dual-Radio 14
1.1.3 Management Mode 15
1.2 Ways to Manage the NWA 15
1.3 Good Habits for Managing the NWA 16
1.4 Hardware Connections 16
1.5 LEDs 17
1.6 Starting and Stopping the NWA 17

Chapter 2
The Web Configurator **19**

2.1 Overview 19
2.2 Access 19
2.3 Navigating the Web Configurator 21
2.3.1 Title Bar 21
2.3.2 Navigation Panel 24
2.3.3 Warning Messages 27
2.3.4 Tables and Lists 27

Part II: Technical Reference **31**

Chapter 3
Dashboard **33**

3.1 Overview 33
3.1.1 What You Can Do in this Chapter 33
3.2 Dashboard 33
3.2.1 CPU Usage 36

3.2.2 Memory Usage 37

Chapter 4
Monitor 39

4.1 Overview 39
4.1.1 What You Can Do in this Chapter 39
4.2 What You Need to Know 39
4.3 LAN Status 40
4.3.1 LAN Status Graph 42
4.4 Radio List 43
4.4.1 AP Mode Radio Information 44
4.5 Station List 45
4.6 Rogue AP 46
4.7 View Log 47

Chapter 5
LAN Setting 51

5.1 Overview 51
5.1.1 What You Can Do in this Chapter 51
5.2 LAN Setting 52

Chapter 6
Wireless 53

6.1 Overview 53
6.1.1 What You Can Do in this Chapter 53
6.1.2 What You Need to Know 54
6.2 AP Management 54
6.3 MON Mode 55
6.3.1 Add/Edit Rogue/Friendly List 57
6.4 Load Balancing 57
6.4.1 Disassociating and Delaying Connections 58
6.5 DCS 60
6.6 Technical Reference 62

Chapter 7
User 65

7.1 Overview 65
7.1.1 What You Can Do in this Chapter 65
7.1.2 What You Need To Know 65
7.2 User Summary 66
7.2.1 Add/Edit User 66
7.3 Setting 68
7.3.1 Edit User Authentication Timeout Settings 70

Chapter 8
AP Profile 73

8.1 Overview 73
8.1.1 What You Can Do in this Chapter 73
8.1.2 What You Need To Know 73
8.2 Radio 74
8.2.1 Add/Edit Radio Profile 76
8.3 SSID 79
8.3.1 SSID List 79
8.3.2 Security List 82
8.3.3 MAC Filter List 86
8.3.4 Layer-2 Isolation List 88

Chapter 9
MON Profile 91

9.1 Overview 91
9.1.1 What You Can Do in this Chapter 91
9.2 MON Profile 91
9.2.1 Add/Edit MON Profile 92
9.3 Technical Reference 93

Chapter 10
Certificates 95

10.1 Overview 95
10.1.1 What You Can Do in this Chapter 95
10.1.2 What You Need to Know 95
10.1.3 Verifying a Certificate 97
10.2 My Certificates 98
10.2.1 Add My Certificates 100
10.2.2 Edit My Certificates 103
10.2.3 Import Certificates 105
10.3 Trusted Certificates 106
10.3.1 Edit Trusted Certificates 108
10.3.2 Import Trusted Certificates 110
10.4 Technical Reference 111

Chapter 11
System 113

11.1 Overview 113
11.1.1 What You Can Do in this Chapter 113
11.2 Host Name 113
11.3 Date and Time 114
11.3.1 Pre-defined NTP Time Servers List 116

11.3.2 Time Server Synchronization 116
11.4 WWW Overview 118
11.4.1 Service Access Limitations 118
11.4.2 System Timeout 118
11.4.3 HTTPS 118
11.4.4 Configuring WWW Service Control 120
11.4.5 HTTPS Example 121
11.5 SSH 128
11.5.1 How SSH Works 129
11.5.2 SSH Implementation on the NWA 130
11.5.3 Requirements for Using SSH 130
11.5.4 Configuring SSH 130
11.5.5 Examples of Secure Telnet Using SSH 131
11.6 Telnet 132
11.7 FTP 133
11.8 SNMP 133
11.8.1 Supported MIBs 135
11.8.2 SNMP Traps 135
11.8.3 Configuring SNMP 135
11.8.4 Adding or Editing an SNMPv3 User Profile 137

Chapter 12
Log and Report 139

12.1 Overview 139
12.1.1 What You Can Do In this Chapter 139
12.2 Email Daily Report 139
12.3 Log Setting 141
12.3.1 Log Setting 142
12.3.2 Edit System Log Settings 143
12.3.3 Edit Remote Server 146
12.3.4 Active Log Summary 147

Chapter 13
File Manager 151

13.1 Overview 151
13.1.1 What You Can Do in this Chapter 151
13.1.2 What you Need to Know 151
13.2 Configuration File 152
13.2.1 Example of Configuration File Download Using FTP 156
13.3 Firmware Package 157
13.3.1 Example of Firmware Upload Using FTP 159
13.4 Shell Script 159

Chapter 14
Diagnostics 163

14.1 Overview 163
14.1.1 What You Can Do in this Chapter 163
14.2 Diagnostics 163

Chapter 15
Reboot 165

15.1 Overview 165
15.1.1 What You Need To Know 165
15.2 Reboot 165

Chapter 16
Shutdown 167

16.1 Overview 167
16.1.1 What You Need To Know 167
16.2 Shutdown 167

Chapter 17
Troubleshooting 169

17.1 Overview 169
17.2 Power, Hardware Connections, and LED 169
17.3 NWA Access and Login 170
17.4 Internet Access 171
17.5 Wireless Connections 172
17.6 Resetting the NWA 175
17.7 Getting More Troubleshooting Help 175

Appendix A Importing Certificates 177

Appendix B Legal Information 191

Index 197

PART I
User's Guide

1

Introduction

1.1 Overview

This User's Guide covers the following models: NWA5121-N, NWA5121-NI, and NWA5123-NI. Your NWA is a wireless AP (Access Point). It extends the range of your existing wired network without additional wiring, providing easy network access to mobile users.

Table 1 NWA Series Comparison Table

FEATURES	NWA5121-N	NWA5121-NI	NWA5123-NI
Supported Wireless Standards	IEEE 802.11b IEEE 802.11g IEEE 802.11n	IEEE 802.11b IEEE 802.11g IEEE 802.11n	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n
Supported Frequency Bands	2.4 GHz	2.4 GHz	2.4 GHz 5 GHz
Available Security Modes	None WEP WPA WPA2 WPA2-MIX WPA-PSK WPA2-PSK WPA2-PSK-MIX	None WEP WPA WPA2 WPA2-MIX WPA-PSK WPA2-PSK WPA2-PSK-MIX	None WEP WPA WPA2 WPA2-MIX WPA-PSK WPA2-PSK WPA2-PSK-MIX
Number of SSID Profiles	32	32	32
Number of Wireless Radios	1	1	2
Layer-2 Isolation	Yes	Yes	Yes
External Antennas	Yes	No	No
Maximum number of log messages	512 event logs or 1024 debug logs		

Your NWA's business-class reliability, SMB features, and centralized wireless management make it ideally suited for advanced service delivery in mission-critical networks. It uses Multiple BSSID and VLAN to provide simultaneous independent virtual APs. Additionally, innovations in roaming technology and QoS features eliminate voice call disruptions. It can serve as an AP, or even as an RF monitor to search for rouge APs to help eliminate network threats.

The NWA controls network access with Media Access Control (MAC) address filtering, and rogue Access Point (AP) detection. It also provides a high level of network traffic security, supporting IEEE 802.1x, Wi-Fi Protected Access (WPA), WPA2 and Wired Equivalent Privacy (WEP) data encryption.

Your NWA is easy to install, configure and use. The embedded Web-based configurator enables simple, straightforward management and maintenance. See the Quick Start Guide for how to make hardware connections.

1.1.1 MBSSID

A Basic Service Set (BSS) is the set of devices forming a single wireless network (usually an access point and one or more wireless clients). The Service Set IDentifier (SSID) is the name of a BSS. In Multiple BSS (MBSSID) mode, the NWA provides multiple virtual APs, each forming its own BSS and using its own individual SSID profile.

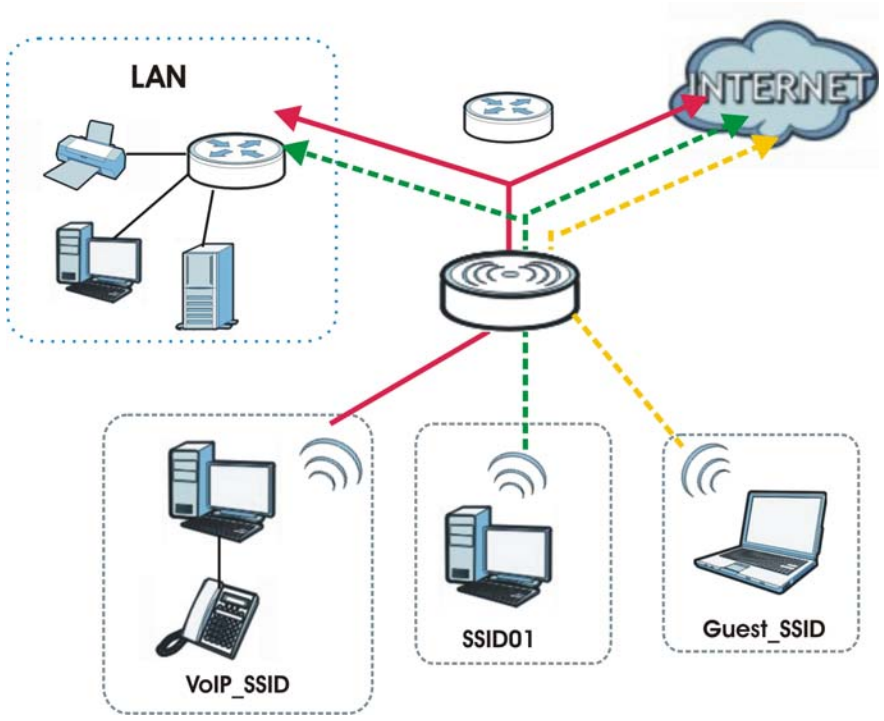
You can configure multiple SSID profiles, and have all of them active at any one time.

You can assign different wireless and security settings to each SSID profile. This allows you to compartmentalize groups of users, set varying access privileges, and prioritize network traffic to and from certain BSSs.

To the wireless clients in the network, each SSID appears to be a different access point. As in any wireless network, clients can associate only with the SSIDs for which they have the correct security settings.

For example, you might want to set up a wireless network in your office where Internet telephony (VoIP) users have priority. You also want a regular wireless network for standard users, as well as a 'guest' wireless network for visitors. In the following figure, **VoIP_SSID** users have QoS priority, **SSID01** is the wireless network for standard users, and **Guest_SSID** is the wireless network for guest users. In this example, the guest user is forbidden access to the wired Land Area Network (LAN) behind the AP and can access only the Internet.

Figure 1 Multiple BSSs



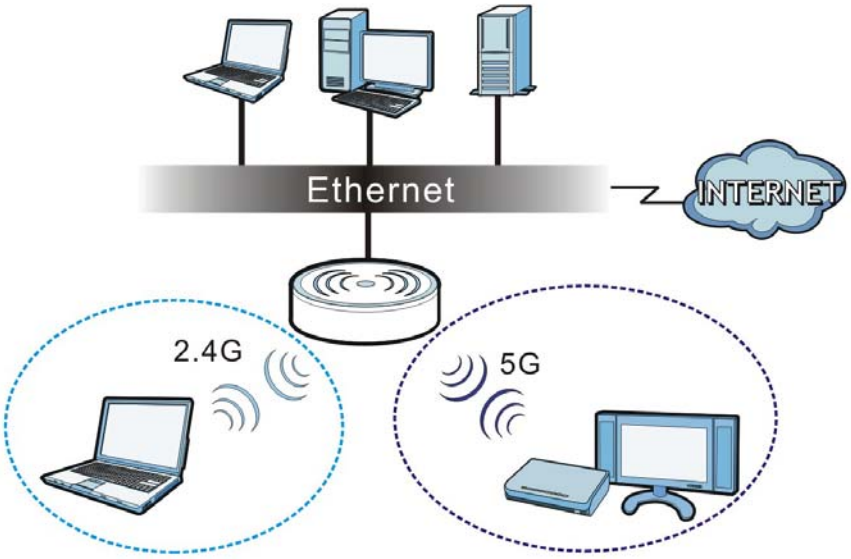
1.1.2 Dual-Radio

The NWA5123-NI is equipped with dual wireless radios. This means you can configure two different wireless networks to operate simultaneously.

Note: A different channel should be configured for each WLAN interface to reduce the effects of radio interference.

You could use the 2.4 GHz band for regular Internet surfing and downloading while using the 5 GHz band for time sensitive traffic like high-definition video, music, and gaming.

Figure 2 Dual-Radio Application



1.1.3 Management Mode

The NWA is a standalone AP by default. You can also switch the NWA from being a standalone AP to acting as a managed AP to allow it to be managed by an AP controller, such as the NXC5200. To change between management modes, you need to have the firmware package for the corresponding mode and upload it to the NWA.

Table 2 NWA Management Mode Comparison

MANAGEMENT MODE	DEFAULT IP ADDRESS	UPLOAD FIRMWARE VIA
Standalone AP	Static (192.168.1.2)	Web Configurator or FTP
Managed AP	Dynamic	FTP

When the NWA is in standalone AP mode, the NWA is set to have a static management IP address (192.168.1.2) by default. You can use either the web configurator or FTP to upload firmware. See Section 13.3 on page 157 for more information about firmware uploading.

When the NWA is in managed AP mode, it acts as a DHCP client and obtains an IP address from the AP controller. It can be configured ONLY by the AP controller. To change the NWA back to standalone AP mode, you need to check the AP controller for the NWA's IP address and use FTP to upload firmware.

1.2 Ways to Manage the NWA

You can use the following ways to manage the NWA.

Web Configurator

The Web Configurator allows easy NWA setup and management using an Internet browser. This User's Guide provides information about the Web Configurator.

Command-Line Interface (CLI)

The CLI allows you to use text-based commands to configure the NWA. You can access it using remote management (for example, SSH or Telnet). See the Command Reference Guide for more information.

File Transfer Protocol (FTP)

This protocol can be used for firmware upgrades and configuration backup and restore.

Simple Network Management Protocol (SNMP)

The NWA can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.

1.3 Good Habits for Managing the NWA

Do the following things regularly to make the NWA more secure and to manage it more effectively.

- Change the password often. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the NWA to its factory default settings. If you backed up an earlier configuration file, you won't have to totally re-configure the NWA; you can simply restore your last configuration.

1.4 Hardware Connections

See your Quick Start Guide for information on making hardware connections.

1.5 LEDs

The following are the LED descriptions for your NWA.

Figure 3 LED

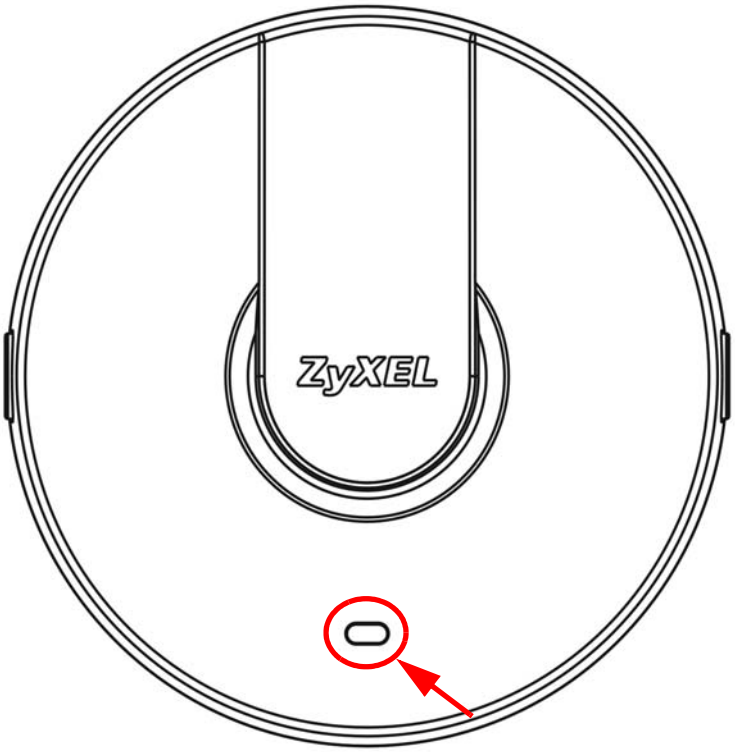


Table 3 LED

COLOR	STATUS	DESCRIPTION
Amber	On	There is system error and the NWA cannot boot up, or the NWA doesn't have an Ethernet connection with the LAN.
	Flashing	The NWA is starting up.
	Off	The NWA is receiving power and ready for use.
Green	On	The WLAN is active.
	Blinking	The WLAN is active, and transmitting or receiving data.
	Off	The WLAN is not active.

1.6 Starting and Stopping the NWA

Here are some of the ways to start and stop the NWA.

Always use Maintenance > Shutdown or the `shutdown` command before you turn off the NWA or remove the power. Not doing so can cause the firmware to become corrupt.

Table 4 Starting and Stopping the NWA

METHOD	DESCRIPTION
Turning on the power	A cold start occurs when you turn on the power to the NWA. The NWA powers up, checks the hardware, and starts the system processes.
Rebooting the NWA	A warm start (without powering down and powering up again) occurs when you use the **Reboot** button in the **Reboot** screen or when you use the `reboot` command. The NWA writes all cached data to the local storage, stops the system processes, and then does a warm start.
Using the RESET button	If you press the **RESET** button, the NWA sets the configuration to its default values and then reboots.
Clicking **Maintenance > Shutdown > Shutdown** or using the `shutdown` command	Clicking **Maintenance > Shutdown > Shutdown** or using the `shutdown` command writes all cached data to the local storage and stops the system processes. Wait for the device to shut down and then manually turn off or remove the power. It does not turn off the power.
Disconnecting the power	Power off occurs when you turn off the power to the NWA. The NWA simply turns off. It does not stop the system processes or write cached data to local storage.

The NWA does not stop or start the system processes when you apply configuration files or run shell scripts although you may temporarily lose access to network resources.

2

The Web Configurator

2.1 Overview

The NWA Web Configurator allows easy management using an Internet browser.

In order to use the Web Configurator, you must:

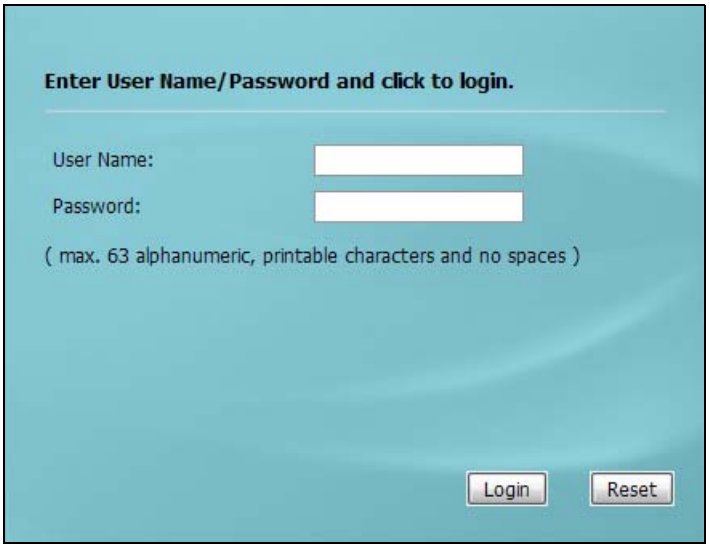
- Use Internet Explorer 7.0 and later or Firefox 1.5 and later
- Allow pop-up windows
- Enable JavaScript (enabled by default)
- Enable Java permissions (enabled by default)
- Enable cookies

The recommended screen resolution is 1024 x 768 pixels and higher.

2.2 Access

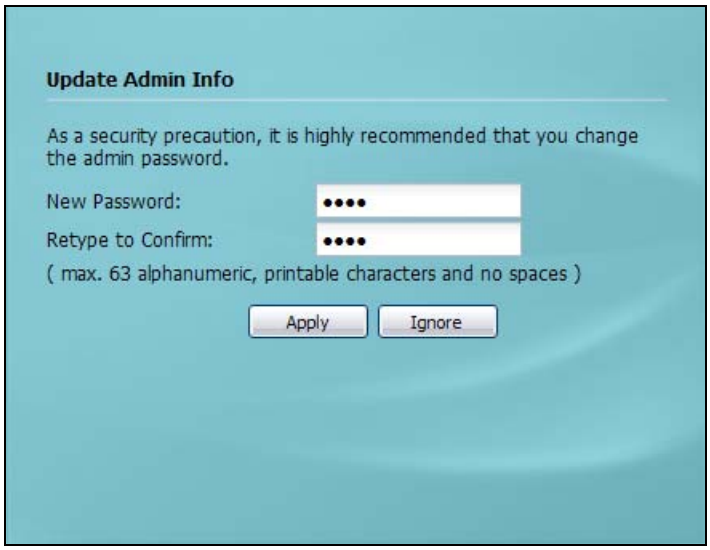
1 Make sure your NWA hardware is properly connected. See the Quick Start Guide.

2 Browse to https://192.168.1.2. The **Login** screen appears.



3 Enter the user name (default: "admin") and password (default: "1234").

4 Click **Login**. If you logged in using the default user name and password, the **Update Admin Info** screen appears. Otherwise, the dashboard appears.

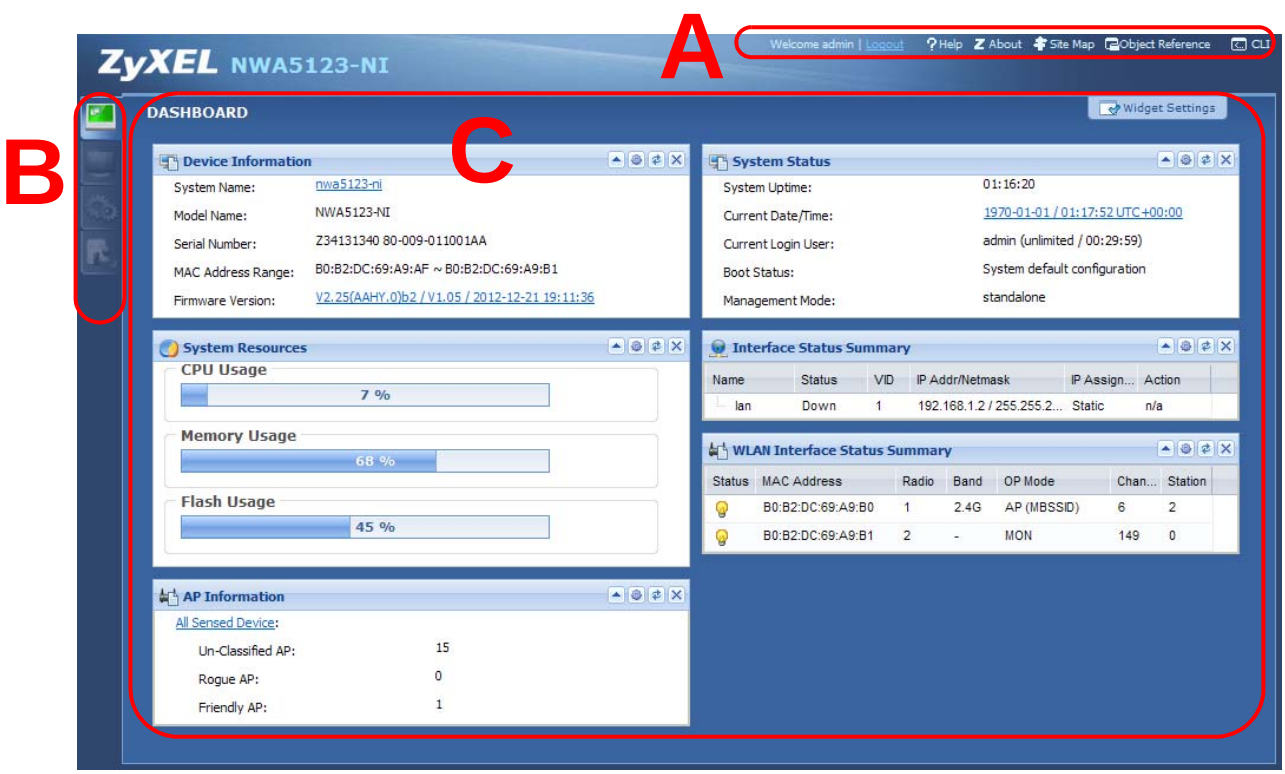

Update Admin Info
As a security precaution, it is highly recommended that you change the admin password.
New Password:
Retype to Confirm:
(max. 63 alphanumeric, printable characters and no spaces)
Apply
Ignore

The **Update Admin Info** screen appears every time you log in using the default user name and default password. If you change the password for the default user account, this screen does not appear anymore.

2.3 Navigating the Web Configurator

The following summarizes how to navigate the web configurator from the **Dashboard** screen. This guide uses the NWA5123-NI screens as an example. The screens may vary slightly for different models.

Figure 4 The Web Configurator's Main Screen



The Web Configurator's main screen is divided into these parts:

- **A** - Title Bar
- **B** - Navigation Panel
- **C** - Main Window

2.3.1 Title Bar

The title bar provides some useful links that always appear over the screens below, regardless of how deep into the Web Configurator you navigate.

Figure 5 Title Bar

The icons provide the following functions.

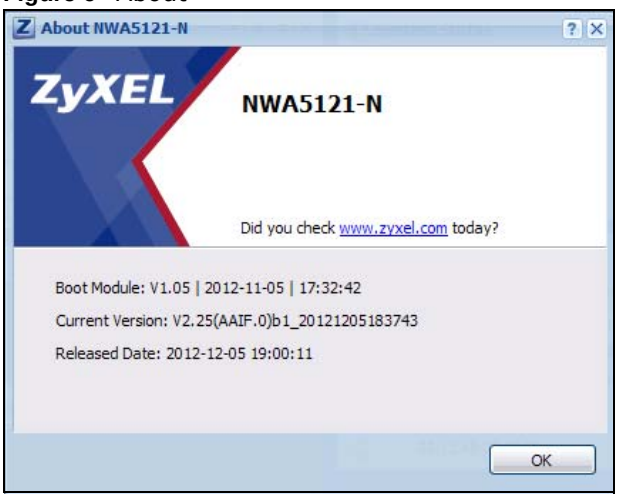
Table 5 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
Logout	Click this to log out of the Web Configurator.
Help	Click this to open the help page for the current screen.
About	Click this to display basic information about the NWA.
Site Map	Click this to see an overview of links to the Web Configurator screens.
Object Reference	Click this to open a screen where you can check which configuration items reference an object.
CLI	Click this to open a popup window that displays the CLI commands sent by the Web Configurator.

About

Click **About** to display basic information about the NWA.

Figure 6 About



The following table describes labels that can appear in this screen.

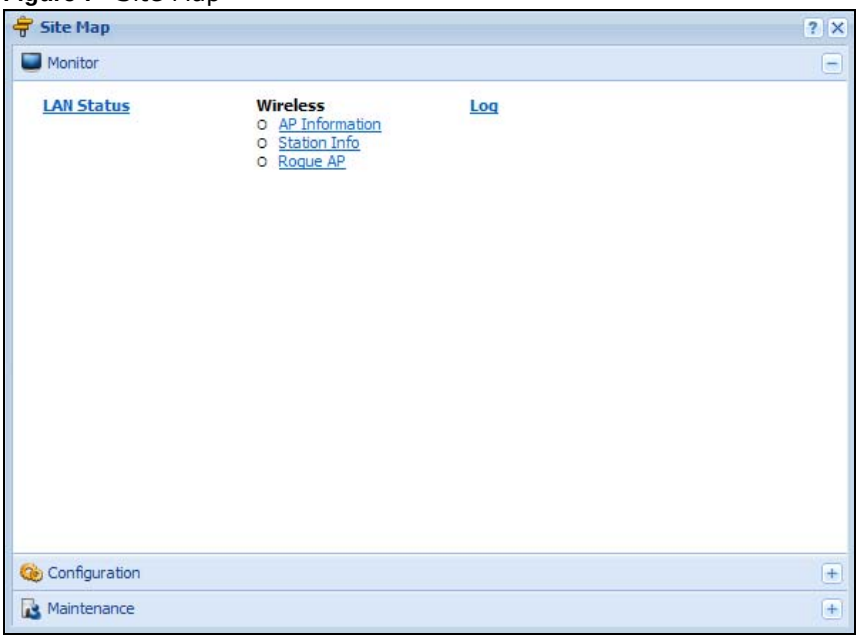
Table 6 About

LABEL	DESCRIPTION
Boot Module	This shows the version number of the software that handles the booting process of the NWA.
Current Version	This shows the firmware version of the NWA.
Released Date	This shows the date (yyyy-mm-dd) and time (hh:mm:ss) when the firmware is released.
OK	Click this to close the screen.

Site Map

Click **Site MAP** to see an overview of links to the Web Configurator screens. Click a screen's link to go to that screen.

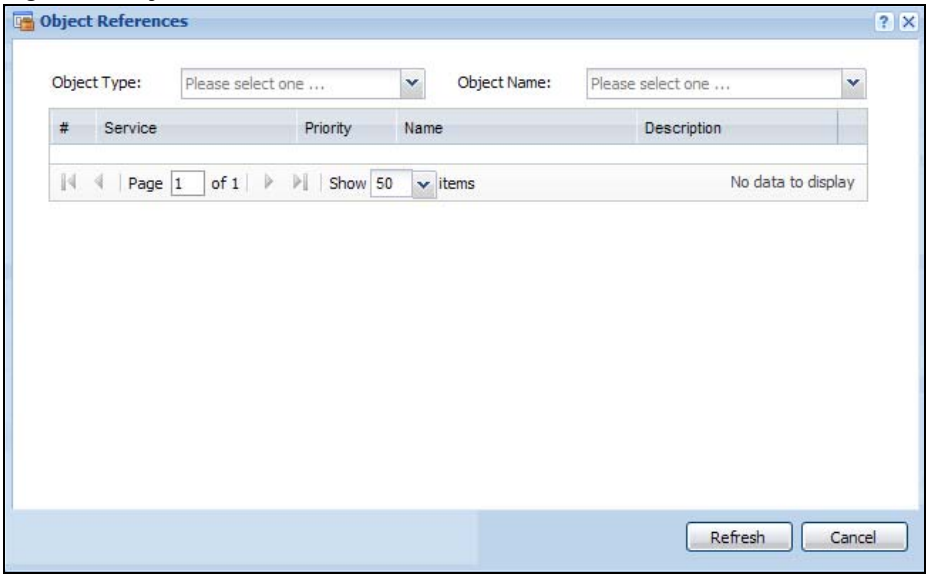
Figure 7 Site Map



Object Reference

Click **Object Reference** to open the **Object Reference** screen. Select the type of object and the individual object and click **Refresh** to show which configuration settings reference the object.

Figure 8 Object Reference



The fields vary with the type of object. The following table describes labels that can appear in this screen.

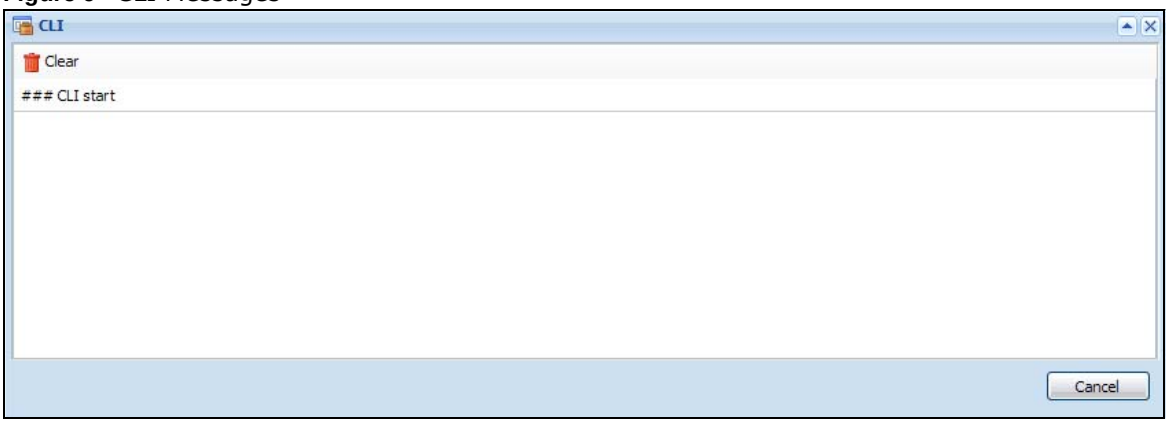
Table 7 Object References

LABEL	DESCRIPTION
Object Name	This identifies the object for which the configuration settings that use it are displayed. Click the object's name to display the object's configuration screen in the main window.
#	This field is a sequential value, and it is not associated with any entry.
Service	This is the type of setting that references the selected object. Click a service's name to display the service's configuration screen in the main window.
Priority	If it is applicable, this field lists the referencing configuration item's position in its list, otherwise **N/A** displays.
Name	This field identifies the configuration item that references the object.
Description	If the referencing configuration item has a description configured, it displays here.
Refresh	Click this to update the information in this screen.
Cancel	Click **Cancel** to close the screen.

CLI Messages

Click **CLI** to look at the CLI commands sent by the Web Configurator. These commands appear in a popup window, such as the following.

Figure 9 CLI Messages



Click **Clear** to remove the currently displayed information.

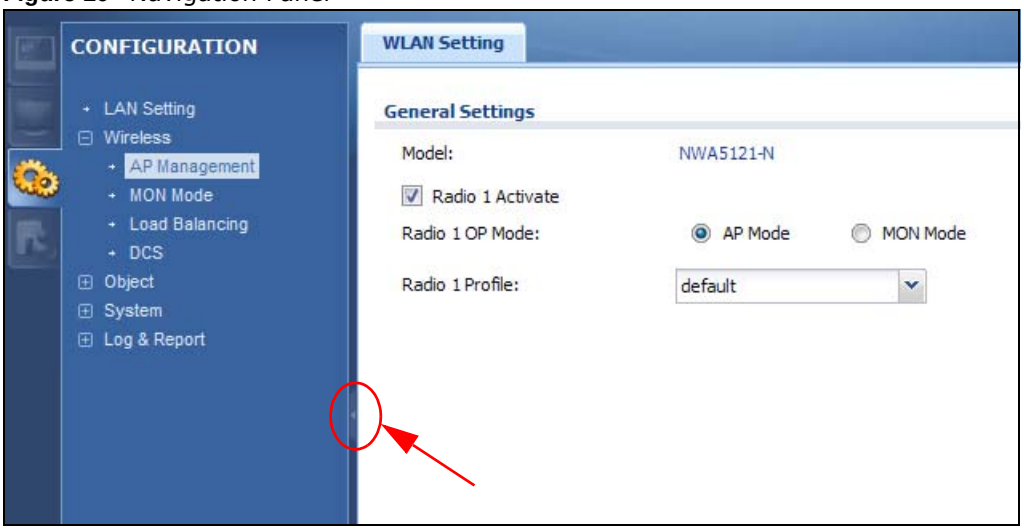
Note: See the Command Reference Guide for information about the commands.

2.3.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure NWA features. Click the arrow in the middle of the right edge of the navigation panel to hide the navigation panel menus or

drag it to resize them. The following sections introduce the NWA's navigation panel menus and their screens.

Figure 10 Navigation Panel



Dashboard

The dashboard displays general device information, system status, system resource usage, and interface status in widgets that you can re-arrange to suit your needs.

For details on the Dashboard's features, see Chapter 3 on page 33.

Monitor Menu

The monitor menu screens display status and statistics information.

Table 8 Monitor Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
LAN Status		Displays general LAN interface information and packet statistics.
Wireless		
AP Info	Radio List	Displays information about the radios of the connected APs.
Station Info		Displays information about the connected stations.
Rogue AP		Displays information about suspected rogue APs.
Log	View Log	Displays log entries for the NWA.

Configuration Menu

Use the configuration menu screens to configure the NWA's features.

Table 9 Configuration Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
LAN Setting		Manage the LAN Ethernet interface including VLAN settings.
Wireless		
AP Management		Edit wireless AP information, remove APs, and reboot them.

Table 9 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
MON Mode		Configure how the NWA monitors for rogue APs.
Load Balancing		Configure load balancing for traffic moving to and from wireless clients.
DCS		Configure dynamic wireless channel selection.
Object		
Users	User	Create and manage users.
	Setting	Manage default settings for all users, general settings for user sessions, and rules to force user authentication.
AP Profile	Radio	Create and manage wireless radio settings files that can be associated with different APs.
	SSID	Create and manage wireless SSID, security, MAC filtering, and layer-2 isolation files that can be associated with different APs.
MON Profile		Create and manage rogue AP monitoring files that can be associated with different APs.
Certificate	My Certificates	Create and manage the NWA's certificates.
	Trusted Certificates	Import and manage certificates from trusted sources.
System		
Host Name		Configure the system and domain name for the NWA.
Date/Time		Configure the current date, time, and time zone in the NWA.
WWW		Configure HTTP, HTTPS, and general authentication.
SSH		Configure SSH server and SSH service settings.
TELNET		Configure telnet server settings for the NWA.
FTP		Configure FTP server settings.
SNMP		Configure SNMP communities and services.
Log & Report		
Email Daily Report		Configure where and how to send daily reports and what reports to send.
Log Setting		Configure the system log, e-mail logs, and remote syslog servers.

Maintenance Menu

Use the maintenance menu screens to manage configuration and firmware files, run diagnostics, and reboot or shut down the NWA.

Table 10 Maintenance Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
File Manager	Configuration File	Manage and upload configuration files for the NWA.
	Firmware Package	View the current firmware version and to upload firmware.
	Shell Script	Manage and run shell script files for the NWA.
Diagnostics	Diagnostic	Collect diagnostic information.
Reboot		Restart the NWA.
Shutdown		Turn off the NWA.

2.3.3 Warning Messages

Warning messages, such as those resulting from misconfiguration, display in a popup window.

Figure 11 Warning Message

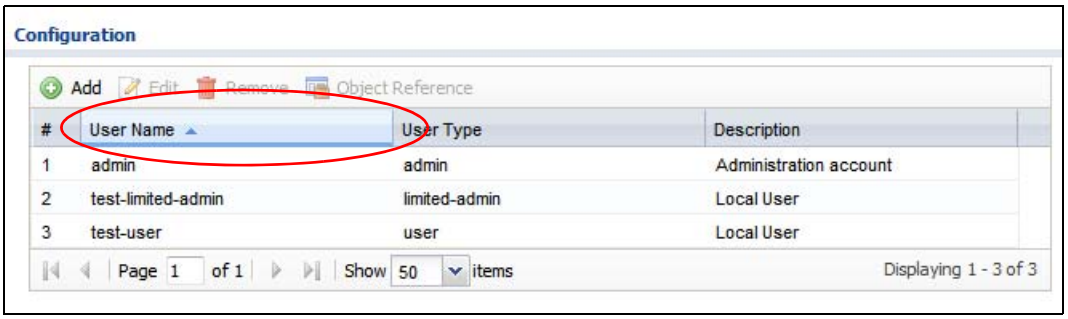
2.3.4 Tables and Lists

The Web Configurator tables and lists are quite flexible and provide several options for how to display their entries.

2.3.4.1 Manipulating Table Display

Here are some of the ways you can manipulate the Web Configurator tables.

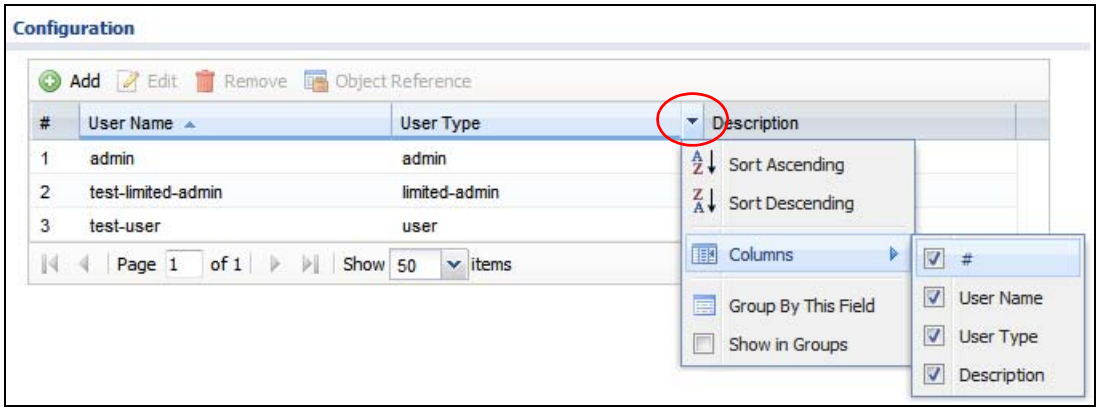
1 Click a column heading to sort the table's entries according to that column's criteria.



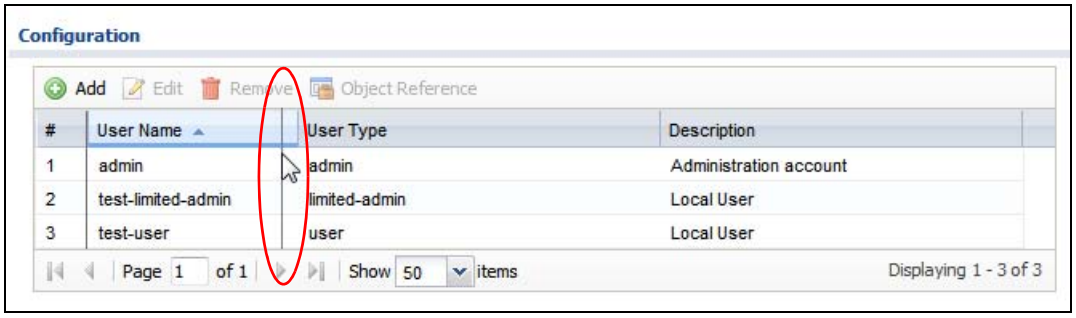
2 Click the down arrow next to a column heading for more options about how to display the entries. The options available vary depending on the type of fields in the column. Here are some examples of what you can do:

- Sort in ascending alphabetical order
- Sort in descending (reverse) alphabetical order
- Select which columns to display
- Group entries by field
- Show entries in groups

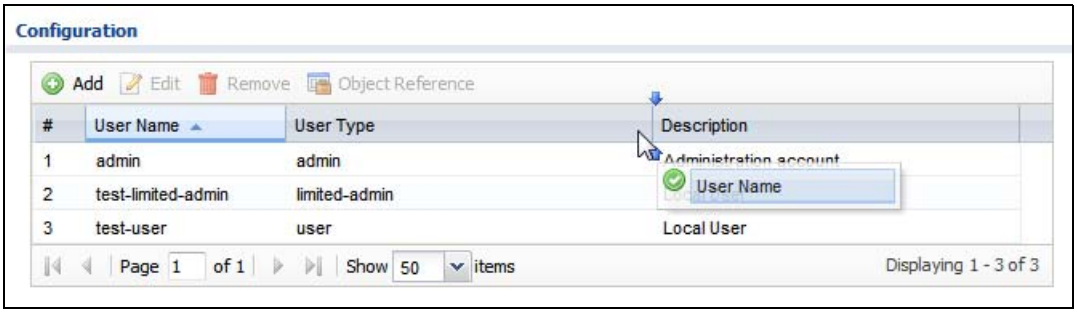
- Filter by mathematical operators (<, >, or =) or searching for text.



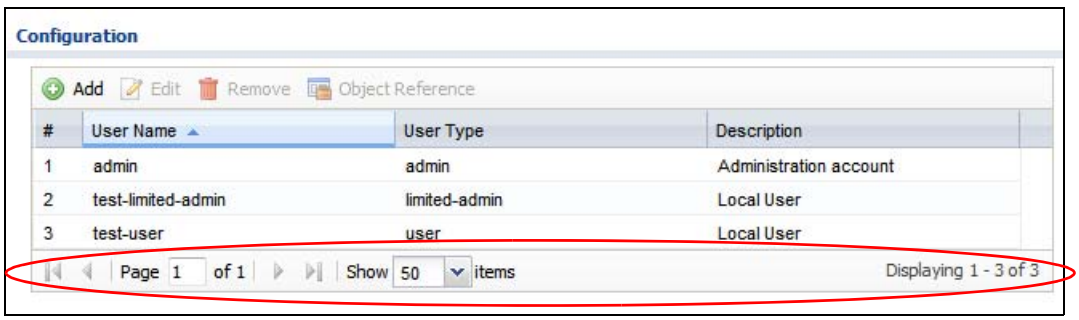
3 Select a column heading cell's right border and drag to re-size the column.



4 Select a column heading and drag and drop it to change the column order. A green check mark displays next to the column's title when you drag the column to a valid new location.



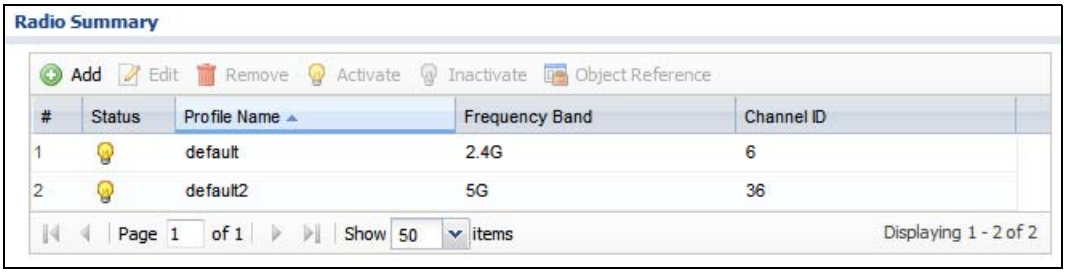
5 Use the icons and fields at the bottom of the table to navigate to different pages of entries and control how many entries display at a time.



2.3.4.2 Working with Table Entries

The tables have icons for working with table entries. A sample is shown next. You can often use the [Shift] or [Ctrl] key to select multiple entries to remove, activate, or deactivate.

Table 11 Common Table Icons



Here are descriptions for the most common table icons.

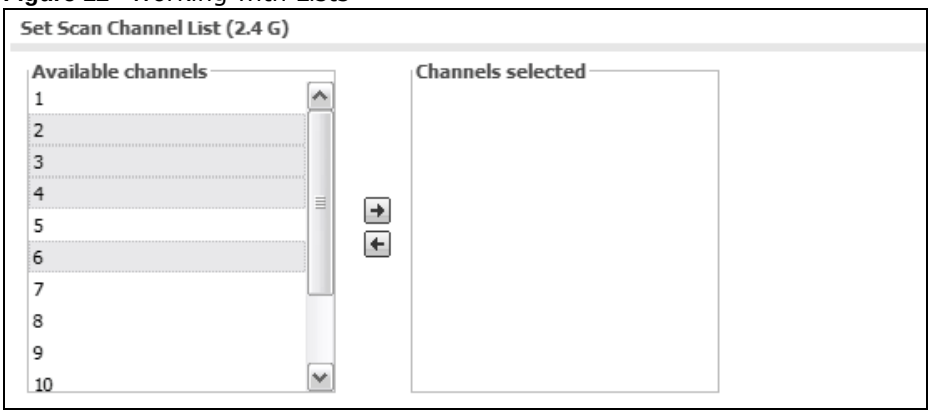
Table 12 Common Table Icons

LABEL	DESCRIPTION
Add	Click this to create a new entry. For features where the entry's position in the numbered list is important (features where the NWA applies the table's entries in order like the firewall for example), you can select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied.
Remove	To remove an entry, select it and click **Remove**. The NWA confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Object Reference	Select an entry and click **Object Reference** to open a screen that shows which settings use the entry.

2.3.4.3 Working with Lists

When a list of available entries displays next to a list of selected entries, you can often just double-click an entry to move it from one list to the other. In some lists you can also use the [Shift] or [Ctrl] key to select multiple entries, and then use the arrow button to move them to the other list.

Figure 12 Working with Lists



PART II
Technical Reference

3

Dashboard

3.1 Overview

Use the **Dashboard** screens to check status information about the NWA.

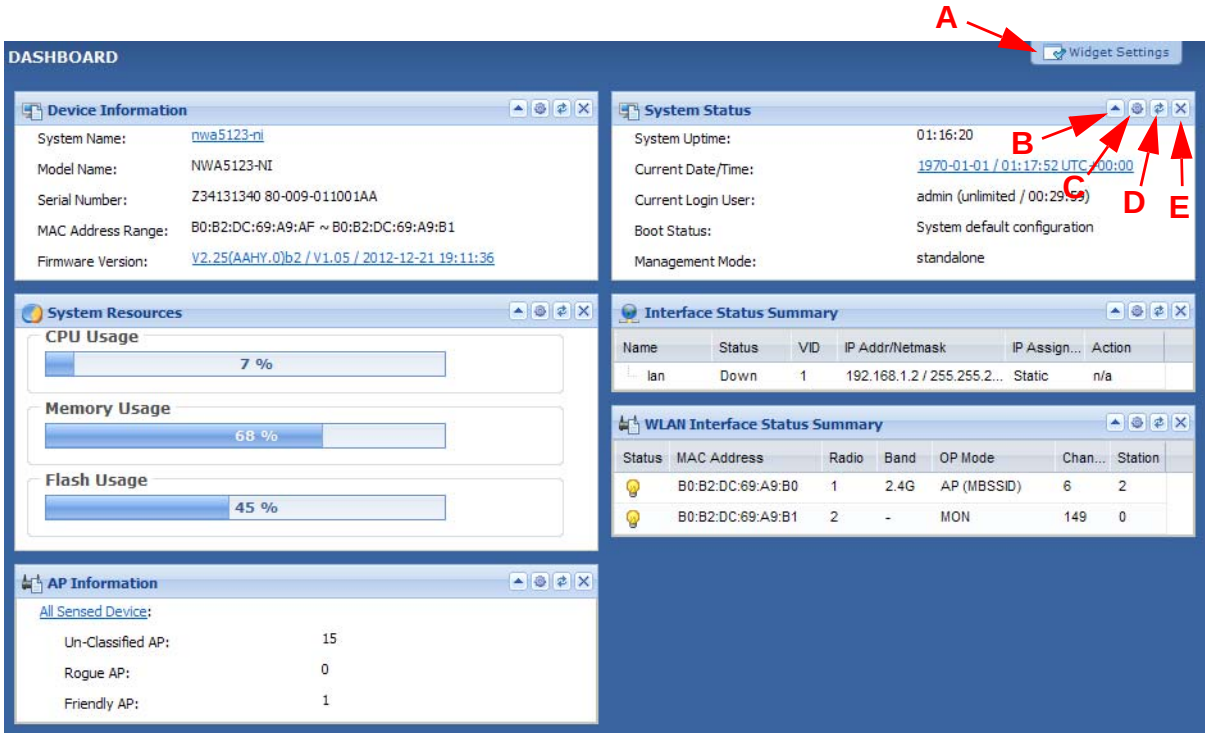
3.1.1 What You Can Do in this Chapter

- The main **Dashboard** screen (Section 3.2 on page 33) displays the NWA's general device information, system status, system resource usage, and interface status. You can also display other status screens for more information.

3.2 Dashboard

This screen is the first thing you see when you log into the NWA. It also appears every time you click the **Dashboard** icon in the navigation panel. The Dashboard displays general device information, system status, system resource usage, and interface status in widgets that you can re-arrange to suit your needs. You can also collapse, refresh, and close individual widgets.

Figure 13 Dashboard



The following table describes the labels in this screen.

Table 13 Dashboard

LABEL	DESCRIPTION
Widget Settings (A)	Use this link to re-open closed widgets. Widgets that are already open appear grayed out.
Up Arrow (B)	Click this to collapse a widget.
Refresh Time Setting (C)	Set the interval for refreshing the information displayed in the widget.
Refresh Now (D)	Click this to update the widget's information immediately.
Close Widget (E)	Click this to close the widget. Use **Widget Setting** to re-open it.
Device Information	
System Name	This field displays the name used to identify the NWA on any network. Click the icon to open the screen where you can change it.
Model Name	This field displays the model name of this NWA.
Serial Number	This field displays the serial number of this NWA.
MAC Address Range	This field displays the MAC addresses used by the NWA. Each physical port or wireless radio has one MAC address. The first MAC address is assigned to the Ethernet LAN port, the second MAC address is assigned to the first radio, and so on.
Firmware Version	This field displays the version number and date of the firmware the NWA is currently running. Click the icon to open the screen where you can upload firmware.
System Resources	
CPU Usage	This field displays what percentage of the NWA's processing capability is currently being used. Hover your cursor over this field to display the **Show CPU Usage** icon that takes you to a chart of the NWA's recent CPU usage.
Memory Usage	This field displays what percentage of the NWA's RAM is currently being used. Hover your cursor over this field to display the **Show Memory Usage** icon that takes you to a chart of the NWA's recent memory usage.
Flash Usage	This field displays what percentage of the NWA's onboard flash memory is currently being used.
AP Information	This shows a summary of connected wireless Access Points (APs).
All Sensed Device	This sections displays a summary of all wireless devices detected by the network.
Un-Classified AP	This displays the number of detected unclassified APs.
Rogue AP	This displays the number of detected rogue APs.
Friendly AP	This displays the number of detected friendly APs.
System Status	
System Uptime	This field displays how long the NWA has been running since it last restarted or was turned on.
Current Date/ Time	This field displays the current date and time in the NWA. The format is yyyy-mm-dd hh:mm:ss.
Current Login User	This field displays the user name used to log in to the current session, the amount of reauthentication time remaining, and the amount of lease time remaining.

Table 13 Dashboard (continued)

LABEL	DESCRIPTION
Boot Status	This field displays details about the NWA's startup state. **OK** - The NWA started up successfully. **Firmware update OK** - A firmware update was successful. **Problematic configuration after firmware update** - The application of the configuration failed after a firmware upgrade. **System default configuration** - The NWA successfully applied the system default configuration. This occurs when the NWA starts for the first time or you intentionally reset the NWA to the system default settings. **Fallback to lastgood configuration** - The NWA was unable to apply the startup-config.conf configuration file and fell back to the lastgood.conf configuration file. **Fallback to system default configuration** - The NWA was unable to apply the lastgood.conf configuration file and fell back to the system default configuration file (system-default.conf). **Booting in progress** - The NWA is still applying the system configuration.
Management Mode	This shows whether the NWA is set to work as a stand alone AP.
Interface Status Summary	If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text. Click the **Detail** icon to go to a (more detailed) summary screen of interface statistics.
Name	This field displays the name of each interface.
Status	This field displays the current status of each interface. The possible values depend on what type of interface it is. **Inactive** - The Ethernet interface is disabled. **Down** - The Ethernet interface is enabled but not connected. **Speed / Duplex** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**).
VID	This field displays the VLAN ID to which the interface belongs.
IP Addr/ Netmask	This field displays the current IP address and subnet mask assigned to the interface. If the IP address is 0.0.0.0, the interface is disabled or did not receive an IP address and subnet mask via DHCP. If this interface is a member of an active virtual router, this field displays the IP address it is currently using. This is either the static IP address of the interface (if it is the master) or the management IP address (if it is a backup).
IP Assignment	This field displays how the interface gets its IP address. **Static** - This interface has a static IP address. **DHCP Client** - This interface gets its IP address from a DHCP server.
Action	If the interface has a static IP address, this shows **n/a**. If the interface has a dynamic IP address, use this field to get or to update the IP address for the interface. Click **Renew** to send a new DHCP request to a DHCP server.
WLAN Interface Status Summary	This displays status information for the WLAN interface.
Status	This displays whether or not the WLAN interface is activated.
MAC Address	This displays the MAC address of the radio.
Radio	This indicates the radio number on the NWA.

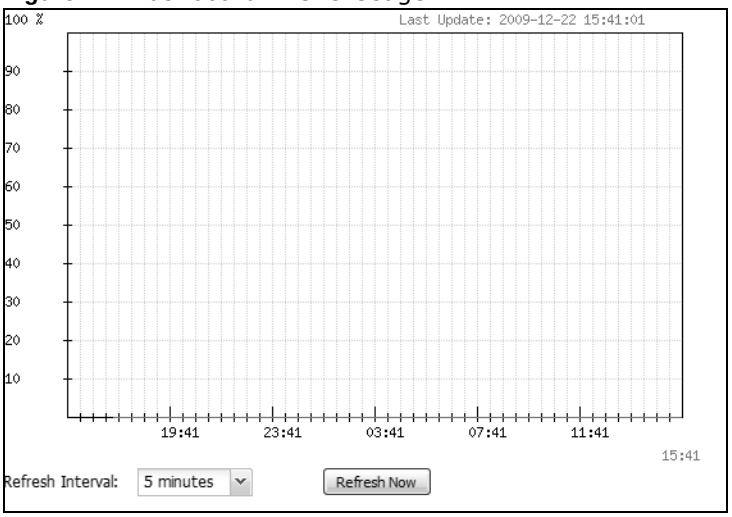
Table 13 Dashboard (continued)

LABEL	DESCRIPTION
Band	This indicates the wireless frequency band currently being used by the radio. This shows **-** when the radio is in monitor mode.
OP Mode	This indicates the radio's operating mode. Operating modes are **AP** (access point), **AP (MBSSID)** or **MON** (monitor).
Channel	This indicates the channel number the radio is using.
Station	This displays the number of wireless clients connected to the NWA.

3.2.1 CPU Usage

Use this screen to look at a chart of the NWA's recent CPU usage. To access this screen, click **CPU Usage** in the dashboard.

Figure 14 Dashboard > CPU Usage



The following table describes the labels in this screen.

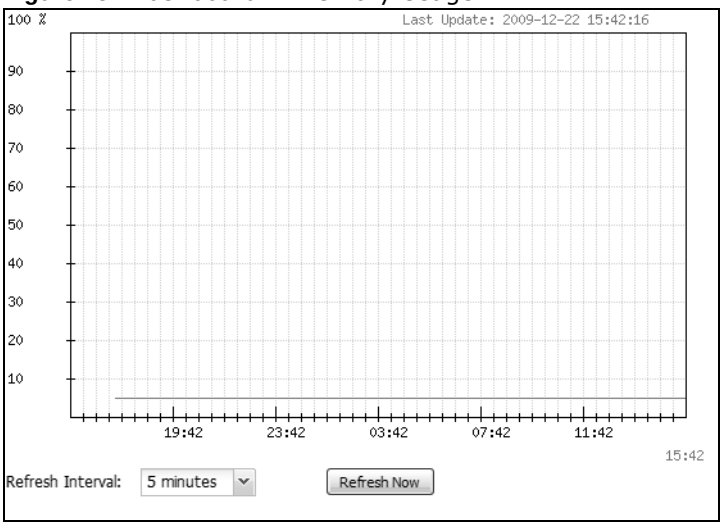
Table 14 Dashboard > CPU Usage

LABEL	DESCRIPTION
%	The y-axis represents the percentage of CPU usage.
time	The x-axis shows the time period over which the CPU usage occurred
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.

3.2.2 Memory Usage

Use this screen to look at a chart of the NWA's recent memory (RAM) usage. To access this screen, click **Memory Usage** in the dashboard.

Figure 15 Dashboard > Memory Usage



The following table describes the labels in this screen.

Table 15 Dashboard > Memory Usage

LABEL	DESCRIPTION
	The y-axis represents the percentage of RAM usage.
	The x-axis shows the time period over which the RAM usage occurred
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.

4

Monitor

4.1 Overview

Use the **Monitor** screens to check status and statistics information.

4.1.1 What You Can Do in this Chapter

- The **LAN Status** screen (Section 4.3 on page 40) displays general LAN interface information and packet statistics.
- The **LAN Status Graph** screen (Section 4.3.1 on page 42) displays a line graph of packet statistics for the NWA's physical LAN port.
- The **Radio List** screen (Section 4.4 on page 43) displays statistics about the wireless radio transmitters in the NWA.
- The **Station Info** screen (Section 4.5 on page 45) displays information about suspected rogue APs.
- The **Rogue AP** screen (Section 4.6 on page 46) displays information about suspected rogue APs.
- The **View Log** screen (Section 4.7 on page 47) displays the NWA's current log messages. You can change the way the log is displayed, you can e-mail the log, and you can also clear the log in this screen.

4.2 What You Need to Know

The following terms and concepts may help as you read through the chapter.

Rogue AP

Rogue APs are wireless access points operating in a network's coverage area that are not under the control of the network's administrators, and can open up holes in a network's security. See Chapter 9 on page 91 for details.

Friendly AP

Friendly APs are other wireless access points that are detected in your network, as well as any others that you know are not a threat (those from neighboring networks, for example). See Chapter 9 on page 91 for details.

4.3 LAN Status

Use this screen to look at general LAN interface information and packet statistics. To access this screen, click **Monitor > LAN Status**.

Figure 16 Monitor > LAN Status

The following table describes the labels in this screen.

Table 16 Monitor > LAN Status

LABEL	DESCRIPTION
Poll Interval	Enter how often you want this window to be updated automatically, and click **Set Interval**.
Set Interval	Click this to set the **Poll Interval** the screen uses.
Stop	Click this to stop the window from updating automatically. You can start it again by setting the **Poll Interval** and clicking **Set Interval**.
Interface Summary	
Name	This field displays the name of the interface.
Status	This field displays the current status of the interface: **Inactive** - The Ethernet interface is disabled. **Down** - The Ethernet interface is enabled but not connected. **Speed / Duplex** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**).
VID	This field displays the VLAN ID to which the interface belongs.
IP Addr/Netmask	This field displays the current IP address and subnet mask assigned to the interface. If the IP address and subnet mask are 0.0.0.0, the interface is disabled or did not receive an IP address and subnet mask via DHCP. If this interface is a member of an active virtual router, this field displays the IP address it is currently using. This is either the static IP address of the interface (if it is the master) or the management IP address (if it is a backup).
IP Assignment	This field displays how the interface gets its IP address. **Static** - This interface has a static IP address. **DHCP Client** - This interface gets its IP address from a DHCP server.

Table 16 Monitor > LAN Status (continued)

LABEL	DESCRIPTION
Action	Use this field to get or to update the IP address for the interface. Click **Renew** to send a new DHCP request to a DHCP server. If the interface cannot use one of these ways to get or to update its IP address, this field displays **n/a**.
Port Statistics Table	
Switch to Graphic View	Click this to display the port statistics as a line graph.
Status	This field displays the current status of the physical port. **Down** - The physical port is not connected. **Speed / Duplex** - The physical port is connected. This field displays the port speed and duplex setting (**Full** or **Half**).
TxPkts	This field displays the number of packets transmitted from the NWA on the physical port since it was last connected.
RxPkts	This field displays the number of packets received by the NWA on the physical port since it was last connected.
Collisions	This field displays the number of collisions on the physical port since it was last connected.
Tx	This field displays the transmission speed, in bytes per second, on the physical port in the one-second interval before the screen updated.
Rx	This field displays the reception speed, in bytes per second, on the physical port in the one-second interval before the screen updated.
Up Time	This field displays how long the physical port has been connected.
System Up Time	This field displays how long the NWA has been running since it last restarted or was turned on.

4.3.1 LAN Status Graph

Use the port statistics graph to look at a line graph of packet statistics for the NWA's physical LAN port. To view, in the **LAN Status** screen click the **Switch to Graphic View** button.

Figure 17 Monitor > LAN Status > Switch to Graphic View

The following table describes the labels in this screen.

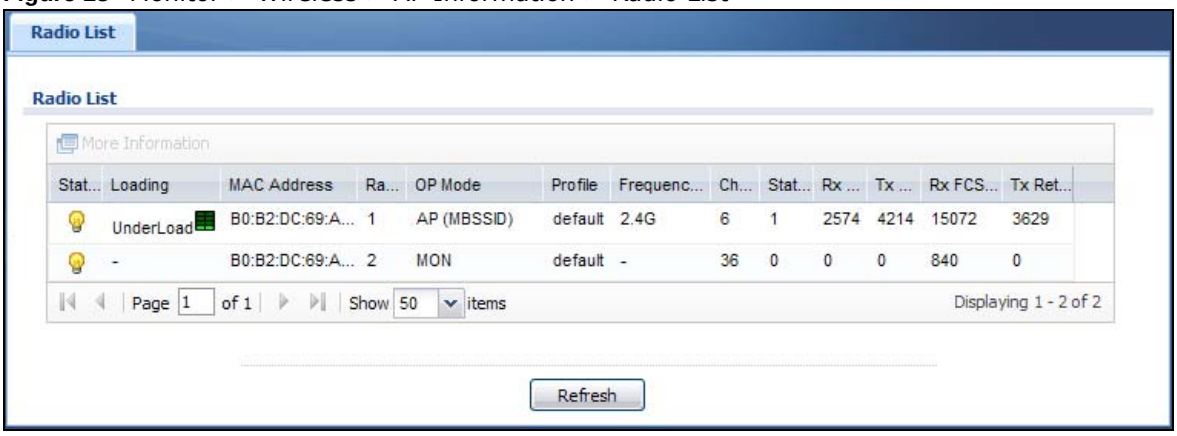
Table 17 Monitor > LAN Status > Switch to Graphic View

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.
Switch to Grid View	Click this to display the port statistics as a table.
bps	The y-axis represents the speed of transmission or reception.
time	The x-axis shows the time period over which the transmission or reception occurred
TX	This line represents traffic transmitted from the NWA on the physical port since it was last connected.
RX	This line represents the traffic received by the NWA on the physical port since it was last connected.
Last Update	This field displays the date and time the information in the window was last updated.

4.4 Radio List

Use this screen to view statistics for the NWA's wireless radio transmitters. To access this screen, click **Monitor > Wireless > AP Information > Radio List**.

Figure 18 Monitor > Wireless > AP Information > Radio List


Radio List
Radio List
More Information
Stat... Loading MAC Address Ra... OP Mode Profile Frequenc... Ch... Stat... Rx ... Tx ... Rx FCS... Tx Ret...
UnderLoad B0:B2:DC:69:A... 1 AP (MBSSID) default 2.4G 6 1 2574 4214 15072 3629
- B0:B2:DC:69:A... 2 MON default - 36 0 0 0 840 0
Page 1 of 1 Show 50 items
Displaying 1 - 2 of 2
Refresh

The following table describes the labels in this screen.

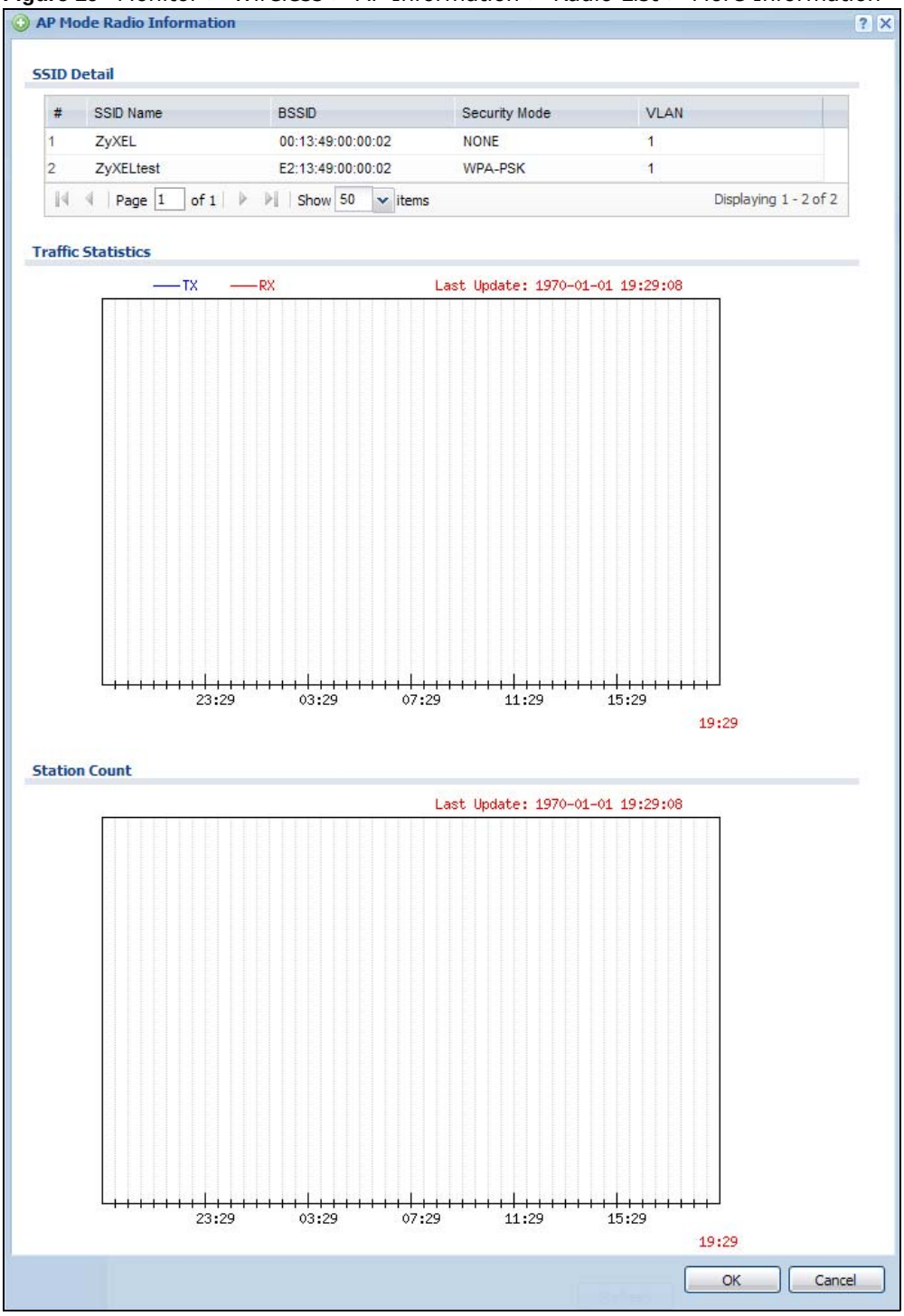
Table 18 Monitor > Wireless > AP Information > Radio List

LABEL	DESCRIPTION
More Information	Click this to view additional information about the selected radio's wireless traffic and station count. Information spans a 24 hour period.
Status	This displays whether or not the radio is enabled.
Loading	This indicates the AP's load balance status (**UnderLoad** or **OverLoad**) when load balancing is enabled on the NWA. Otherwise, it shows **-** when load balancing is disabled or the radio is in monitor mode.
MAC Address	This displays the MAC address of the radio.
Radio	This indicates the radio number on the NWA to which it belongs.
OP Mode	This indicates the radio's operating mode. Operating modes are **AP** (access point), **AP (MBSSID)** or **MON** (monitor).
Profile	This indicates the AP profile name to which the radio belongs.
Frequency Band	This indicates the wireless frequency band currently being used by the radio. This shows **-** when the radio is in monitor mode.
Channel ID	This indicates the radio's channel ID.
Station	This displays the number of wireless clients connected to this radio on the NWA.
Rx PKT	This displays the total number of packets received by the radio.
Tx PKT	This displays the total number of packets transmitted by the radio.
Rx FCS Error Count	This indicates the number of received packet errors accrued by the radio.
Tx Retry Count	This indicates the number of times the radio has attempted to re-transmit packets.

4.4.1 AP Mode Radio Information

This screen allows you to view a selected radio's SSID details, wireless traffic statistics and station count for the preceding 24 hours. To access this window, select a radio and click the **More Information** button in the **Radio List** screen.

Figure 19 Monitor > Wireless > AP Information > Radio List > More Information


AP Mode Radio Information
SSID Detail
SSID Name BSSID Security Mode VLAN
1 ZyXEL 00:13:49:00:00:02 NONE 1
2 ZyXELtest E2:13:49:00:00:02 WPA-PSK 1
Page 1 of 1 Show 50 items Displaying 1 - 2 of 2
Traffic Statistics
TX RX Last Update: 1970-01-01 19:29:08
23:29 03:29 07:29 11:29 15:29 19:29
Station Count
Last Update: 1970-01-01 19:29:08
23:29 03:29 07:29 11:29 15:29 19:29
OK Cancel

The following table describes the labels in this screen.

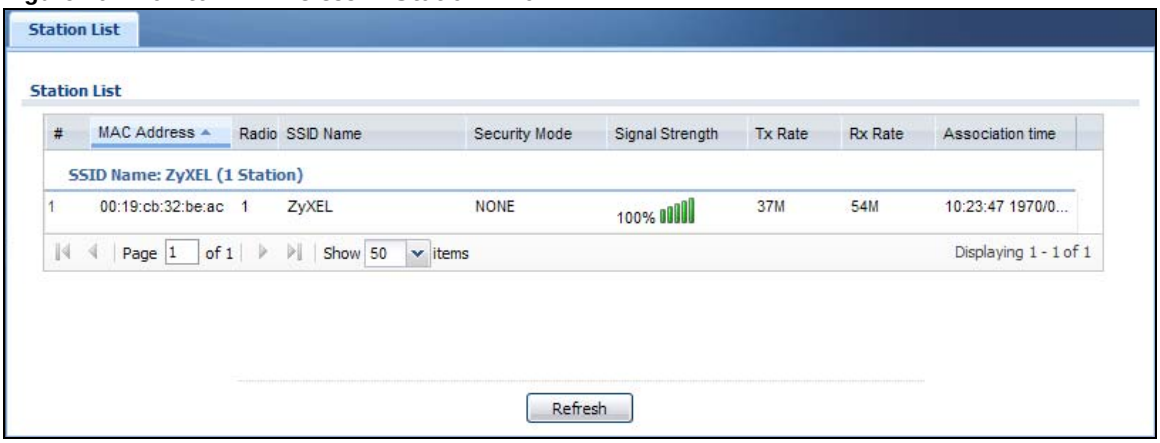
Table 19 Monitor > Wireless > AP Information > Radio List > More Information

LABEL	DESCRIPTION
SSID Detail	This list shows information about all the wireless clients that have connected to the specified radio over the preceding 24 hours.
#	This is the items sequential number in the list. It has no bearing on the actual data in this list.
SSID Name	This displays an SSID associated with this radio. There can be up to eight maximum.
BSSID	This displays a BSSID associated with this radio. The BSSID is tied to the SSID.
Security Mode	This displays the security mode in which the SSID is operating.
VLAN	This displays the VLAN ID associated with the SSID.
Traffic Statistics	This graph displays the overall traffic information of the radio over the preceding 24 hours.
	This y-axis represents the amount of data moved across this radio in megabytes per second.
	This x-axis represents the amount of time over which the data moved across this radio.
Station Count	This graph displays the connected station information of the radio over the preceding 24 hours
	The y-axis represents the number of connected stations.
	The x-axis shows the time period over which a station was connected.
Last Update	This field displays the date and time the information in the window was last updated.
OK	Click this to close this window.
Cancel	Click this to close this window.

4.5 Station List

Use this screen to view statistics pertaining to the associated stations (or "wireless clients"). Click **Monitor > Wireless > Station Info** to access this screen.

Figure 20 Monitor > Wireless > Station Info


Station List
Station List
MAC Address Radio SSID Name Security Mode Signal Strength Tx Rate Rx Rate Association time
SSID Name: ZyXEL (1 Station)
1 00:19:cb:32:be:ac 1 ZyXEL NONE 100% 37M 54M 10:23:47 1970/0...
Page 1 of 1 Show 50 items
Displaying 1 - 1 of 1
Refresh

The following table describes the labels in this screen.

Table 20 Monitor > Wireless > Station Info

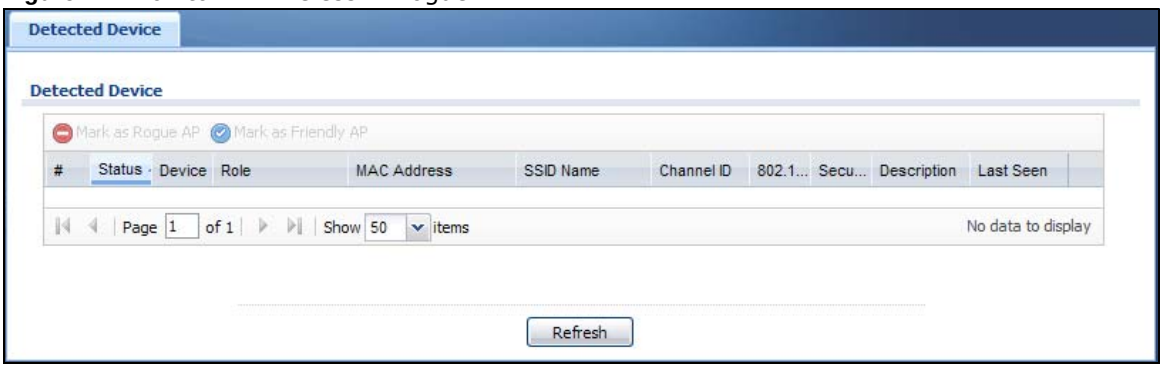
LABEL	DESCRIPTION
#	This is the station's index number in this list.
MAC Address	This is the station's MAC address.
Radio	This is the radio number on the NWA to which the station is connected.
SSID Name	This indicates the name of the wireless network to which the station is connected. A single AP can have multiple SSIDs or networks.
Security Mode	This indicates which secure encryption methods is being used by the station to connect to the network.
Signal Strength	This is the RSSI (Received Signal Strength Indicator) of the station's wireless connection.
Tx Rate	This is the maximum transmission rate of the station.
Rx Rate	This is the maximum reception rate of the station.
Association Time	This displays the time the station first associated with the NWA's wireless network.
Refresh	Click this to refresh the items displayed on this page.

4.6 Rogue AP

Use this screen to view information about suspected rogue APs. Click **Monitor > Wireless > Rogue AP > Detected Device** to access this screen.

Note: The radio or at least one of the NWA's radio must be set to monitor mode (in the **Wireless > AP Management** screen) in order to detect other wireless devices in its vicinity.

Figure 21 Monitor > Wireless > Rogue AP


Detected Device
Detected Device
Mark as Rogue AP
Mark as Friendly AP
Status Device Role MAC Address SSID Name Channel ID 802.1... Secu... Description Last Seen
Page 1 of 1 Show 50 items
No data to display
Refresh

The following table describes the labels in this screen.

Table 21 Monitor > Wireless > Rogue AP

LABEL	DESCRIPTION
Mark as Rogue AP	Click this button to mark the selected AP as a rogue AP. A rogue AP can be contained in the **Configuration > Wireless > MON Mode** screen (Section 6.3 on page 55).
Mark as Friendly AP	Click this button to mark the selected AP as a friendly AP. For more on managing friendly APs, see the **Configuration > Wireless > MON Mode** screen (Section 6.3 on page 55).
#	This is the detected device's index number in this list.

Table 21 Monitor > Wireless > Rogue AP (continued)

LABEL	DESCRIPTION
Status	This indicates the detected device's status.
Device	This indicates the type of device detected.
Role	This indicates the detected device's role (such as friendly or rogue).
MAC Address	This indicates the detected device's MAC address.
SSID Name	This indicates the detected device's SSID.
Channel ID	This indicates the detected device's channel ID.
802.11 Mode	This indicates the 802.11 mode (a/b/g/n) transmitted by the detected device.
Security	This indicates the encryption method (if any) used by the detected device.
Description	This displays the detected device's description. For more on managing friendly and rogue APs, see the **Configuration > Wireless > MON Mode** screen (Section 6.3 on page 55).
Last Seen	This indicates the last time the device was detected by the NWA.
Refresh	Click this to refresh the items displayed on this page.

4.7 View Log

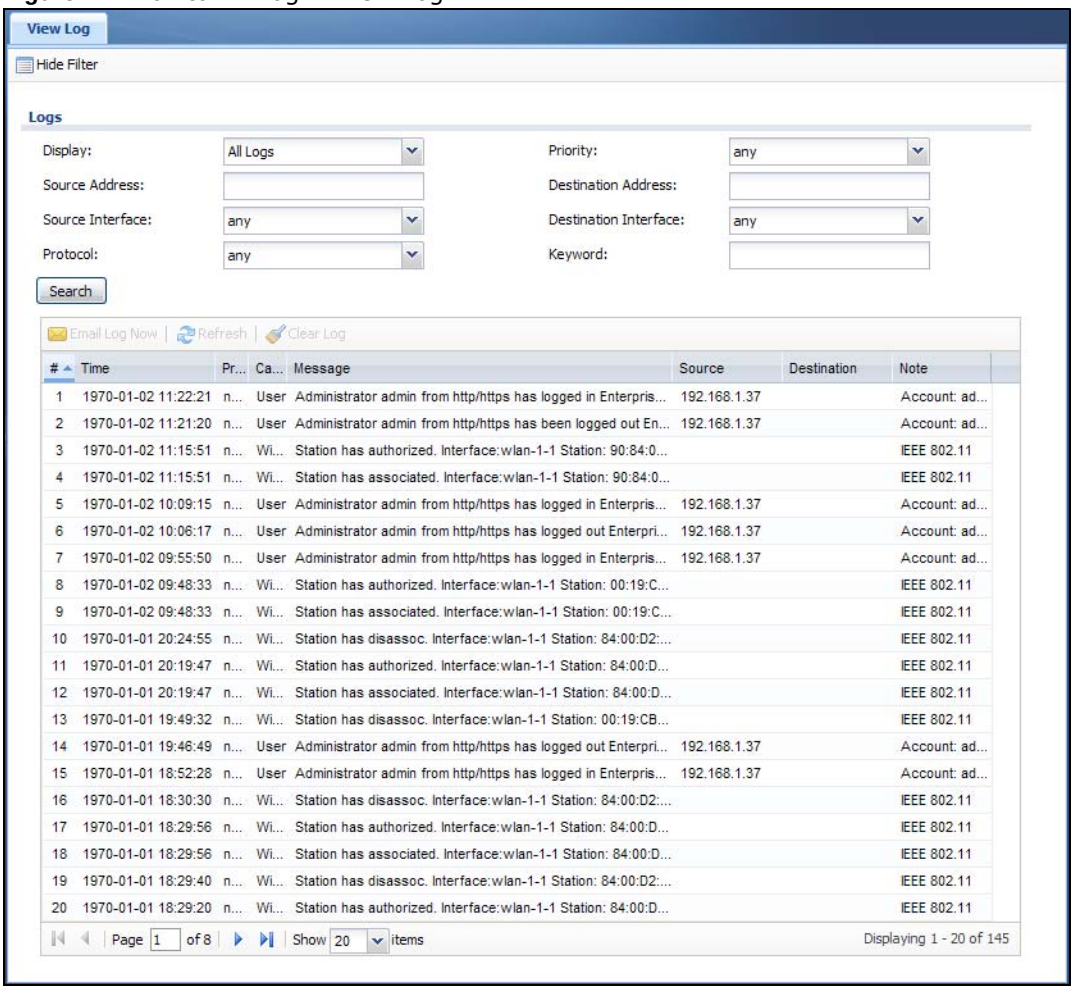
Log messages are stored in two separate logs, one for regular log messages and one for debugging messages. In the regular log, you can look at all the log messages by selecting **All Logs**, or you can select a specific category of log messages (for example, user). You can also look at the debugging log by selecting **Debug Log**. All debugging messages have the same priority.

To access this screen, click **Monitor > Log**. The log is displayed in the following screen.

Note: When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

Events that generate an alert (as well as a log message) display in red. Regular logs display in black. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 22 Monitor > Log > View Log


View Log
Hide Filter
Logs
Display: All Logs
Priority: any
Source Address:
Destination Address:
Source Interface: any
Destination Interface: any
Protocol: any
Keyword:
Search
Email Log Now | Refresh | Clear Log
Time Pr... Ca... Message Source Destination Note
1 1970-01-02 11:22:21 n... User Administrator admin from http/https has logged in Enterpris... 192.168.1.37 Account: ad...
2 1970-01-02 11:21:20 n... User Administrator admin from http/https has been logged out En... 192.168.1.37 Account: ad...
3 1970-01-02 11:15:51 n... Wi... Station has authorized. Interface:wlan-1-1 Station: 90:84:0... IEEE 802.11
4 1970-01-02 11:15:51 n... Wi... Station has associated. Interface:wlan-1-1 Station: 90:84:0... IEEE 802.11
5 1970-01-02 10:09:15 n... User Administrator admin from http/https has logged in Enterpris... 192.168.1.37 Account: ad...
6 1970-01-02 10:06:17 n... User Administrator admin from http/https has logged out Enterpri... 192.168.1.37 Account: ad...
7 1970-01-02 09:55:50 n... User Administrator admin from http/https has logged in Enterpris... 192.168.1.37 Account: ad...
8 1970-01-02 09:48:33 n... Wi... Station has authorized. Interface:wlan-1-1 Station: 00:19:C... IEEE 802.11
9 1970-01-02 09:48:33 n... Wi... Station has associated. Interface:wlan-1-1 Station: 00:19:C... IEEE 802.11
10 1970-01-01 20:24:55 n... Wi... Station has disassoc. Interface:wlan-1-1 Station: 84:00:D2:... IEEE 802.11
11 1970-01-01 20:19:47 n... Wi... Station has authorized. Interface:wlan-1-1 Station: 84:00:D... IEEE 802.11
12 1970-01-01 20:19:47 n... Wi... Station has associated. Interface:wlan-1-1 Station: 84:00:D... IEEE 802.11
13 1970-01-01 19:49:32 n... Wi... Station has disassoc. Interface:wlan-1-1 Station: 00:19:CB... IEEE 802.11
14 1970-01-01 19:46:49 n... User Administrator admin from http/https has logged out Enterpri... 192.168.1.37 Account: ad...
15 1970-01-01 18:52:28 n... User Administrator admin from http/https has logged in Enterpris... 192.168.1.37 Account: ad...
16 1970-01-01 18:30:30 n... Wi... Station has disassoc. Interface:wlan-1-1 Station: 84:00:D2:... IEEE 802.11
17 1970-01-01 18:29:56 n... Wi... Station has authorized. Interface:wlan-1-1 Station: 84:00:D... IEEE 802.11
18 1970-01-01 18:29:56 n... Wi... Station has associated. Interface:wlan-1-1 Station: 84:00:D... IEEE 802.11
19 1970-01-01 18:29:40 n... Wi... Station has disassoc. Interface:wlan-1-1 Station: 84:00:D2:... IEEE 802.11
20 1970-01-01 18:29:20 n... Wi... Station has authorized. Interface:wlan-1-1 Station: 84:00:D... IEEE 802.11
Page 1 of 8 Show 20 items
Displaying 1 - 20 of 145

The following table describes the labels in this screen.

Table 22 Monitor > Log > View Log

LABEL	DESCRIPTION
Show Filter / Hide Filter	Click this button to show or hide the filter settings. If the filter settings are hidden, the **Display**, **Email Log Now**, **Refresh**, and **Clear Log** fields are available. If the filter settings are shown, the **Display**, **Priority**, **Source Address**, **Destination Address**, **Service**, **Keyword**, and **Search** fields are available.
Display	Select the category of log message(s) you want to view. You can also view **All Logs** at one time, or you can view the **Debug Log**.
Priority	This displays when you show the filter. Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices are: **any**, **emerg**, **alert**, **crit**, **error**, **warn**, **notice**, and **info**, from highest priority to lowest priority. This field is read-only if the **Category** is **Debug Log**.
Source Address	This displays when you show the filter. Type the source IP address of the incoming packet that generated the log message. Do not include the port in this filter.

Table 22 Monitor > Log > View Log (continued)

LABEL	DESCRIPTION
Destination Address	This displays when you show the filter. Type the IP address of the destination of the incoming packet when the log message was generated. Do not include the port in this filter.
Source Interface	This displays when you show the filter. Select the source interface of the packet that generated the log message.
Destination Interface	This displays when you show the filter. Select the destination interface of the packet that generated the log message.
Protocol	This displays when you show the filter. Select a service protocol whose log messages you would like to see.
Keyword	This displays when you show the filter. Type a keyword to look for in the **Message**, **Source**, **Destination** and **Note** fields. If a match is found in any field, the log message is displayed. You can use up to 63 alphanumeric characters and the underscore, as well as punctuation marks ()' ,:;?! +-*/= #$% @ ; the period, double quotes, and brackets are not allowed.
Search	This displays when you show the filter. Click this button to update the log using the current filter settings.
Email Log Now	Click this button to send log messages to the **Active** e-mail addresses specified in the **Send Log To** field on the **Configuration > Log & Report > Log Settings** screen.
Refresh	Click this to update the list of logs.
Clear Log	Click this button to clear the whole log, regardless of what is currently displayed on the screen.
#	This field is a sequential value, and it is not associated with a specific log message.
Time	This field displays the time the log message was recorded.
Priority	This field displays the priority of the log message. It has the same range of values as the **Priority** field above.
Category	This field displays the log that generated the log message. It is the same value used in the **Display** and (other) **Category** fields.
Message	This field displays the reason the log message was generated. The text "[count=*x*]", where *x* is a number, appears at the end of the **Message** field if log consolidation is turned on and multiple entries were aggregated to generate into this one.
Source	This field displays the source IP address and the port number in the event that generated the log message.
Destination	This field displays the destination IP address and the port number of the event that generated the log message.
Note	This field displays any additional information about the log message.

The Web Configurator saves the filter settings if you leave the **View Log** screen and return to it later.

5

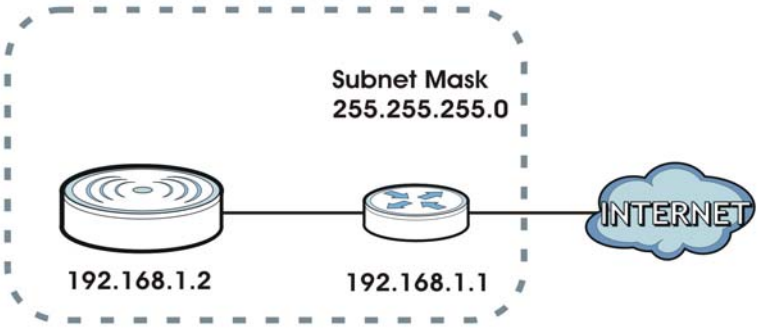
LAN Setting

5.1 Overview

This chapter describes how you can configure the management IP address of your NWA.

The Internet Protocol (IP) address identifies a device on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Figure 23 IP Setup



The figure above illustrates one possible setup of your NWA. The gateway IP address is 192.168.1.1 and the IP address of the NWA is 192.168.1.2 (default). The gateway and the NWA must belong in the same subnet mask to be able to communicate with each other.

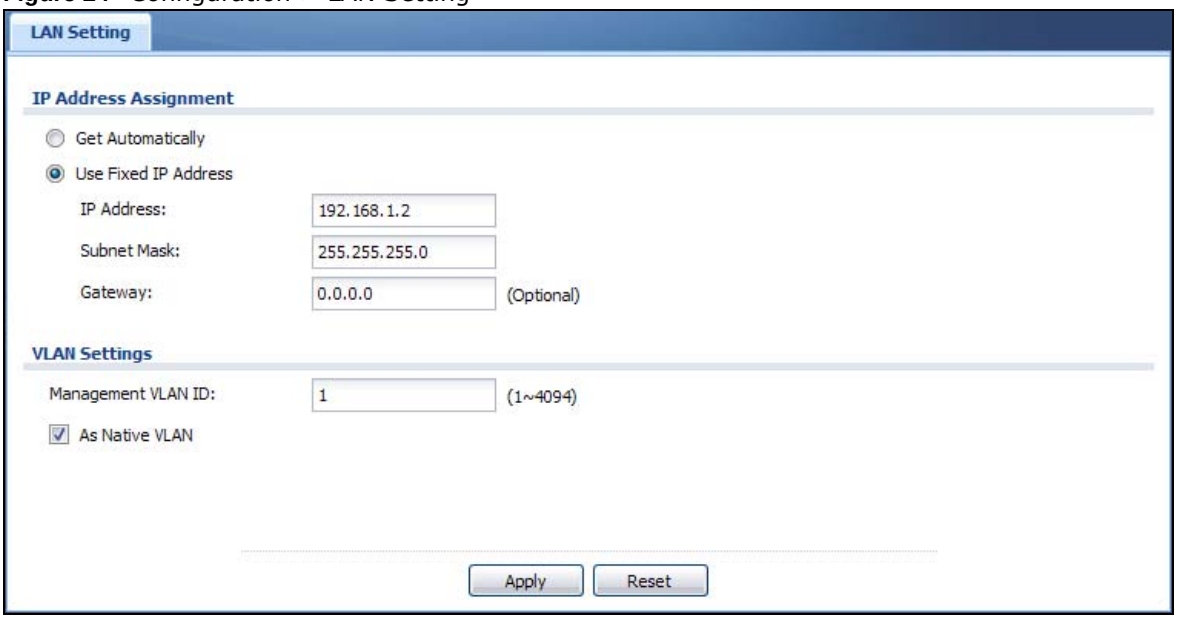
5.1.1 What You Can Do in this Chapter

The **LAN Setting** screen (Section 5.2 on page 52) configures the NWA's LAN IP address and VLAN settings.

5.2 LAN Setting

Use this screen to configure the IP address for your NWA. To access this screen, click **Configuration > LAN Setting**.

Figure 24 Configuration > LAN Setting



Each field is described in the following table.

Table 23 Configuration > LAN Setting

LABEL	DESCRIPTION
IP Address Assignment	
Get Automatically	Select this to make the interface a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	Enter the IP address of the gateway. The NWA sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
VLAN Settings	
Management VLAN ID	Enter a VLAN ID for the NWA.
As Native VLAN	Select this option to treat this VLAN ID as a VLAN created on the NWA and not one assigned to it from outside the network.
Apply	Click **Apply** to save your changes back to the NWA.
Reset	Click **Reset** to return the screen to its last-saved settings.

6

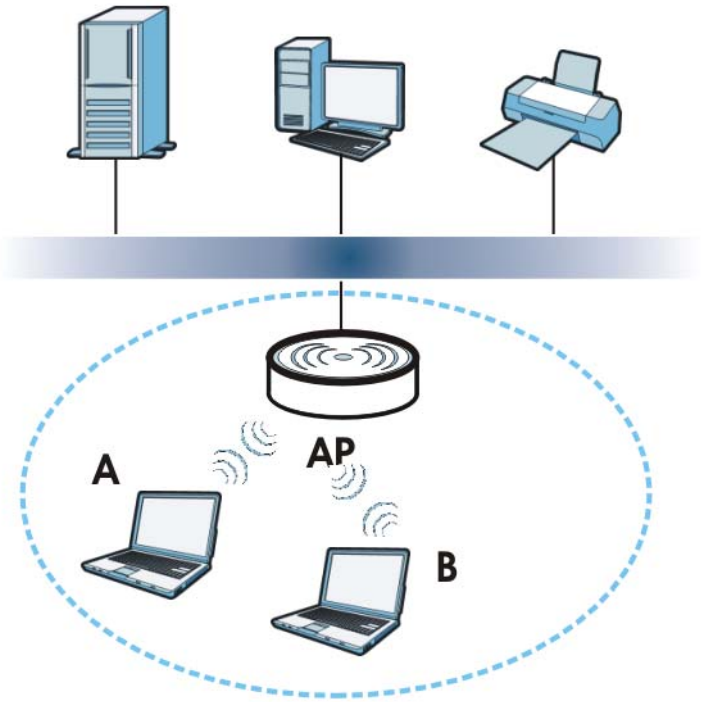
Wireless

6.1 Overview

This chapter discusses how to configure the wireless network settings in your NWA.

The following figure provides an example of a wireless network.

Figure 25 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your NWA is the AP.

6.1.1 What You Can Do in this Chapter

- The **AP Management** screen (Section 6.2 on page 54) manages the NWA's general wireless settings.
- The **MON Mode** screen (Section 6.3 on page 55) allows you to assign APs either to the rogue AP list or the friendly AP list.
- The **Load Balancing** screen (Section 6.4 on page 57) configures network traffic load balancing between the APs and the NWA.
- The **DCS** screen (Section 6.5 on page 60) configures dynamic radio channel selection.

6.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

Station / Wireless Client

A station or wireless client is any wireless-capable device that can connect to an AP using a wireless signal.

Dynamic Channel Selection (DCS)

Dynamic Channel Selection (DCS) is a feature that allows an AP to automatically select the radio channel upon which it broadcasts by scanning the area around it and determining what channels are currently being used by other devices.

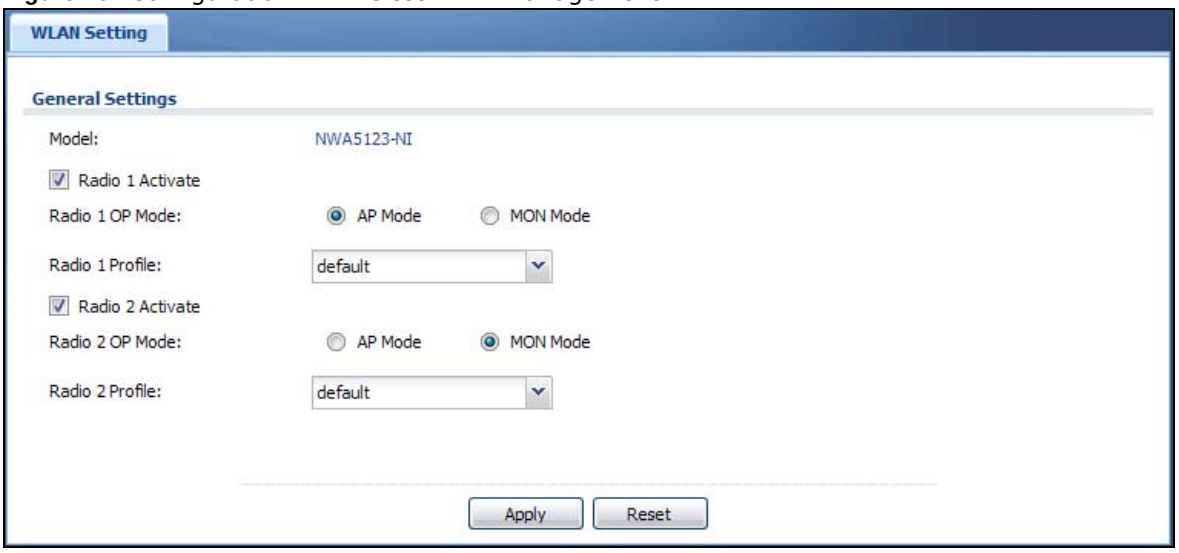
Load Balancing (Wireless)

Wireless load balancing is the process where you limit the number of connections allowed on an wireless access point (AP) or you limit the amount of wireless traffic transmitted and received on it so the AP does not become overloaded.

6.2 AP Management

Use this screen to manage the NWA's general wireless settings. Click **Configuration > Wireless > AP Management** to access this screen.

Figure 26 Configuration > Wireless > AP Management



Each field is described in the following table.

Table 24 Configuration > Wireless > AP Management

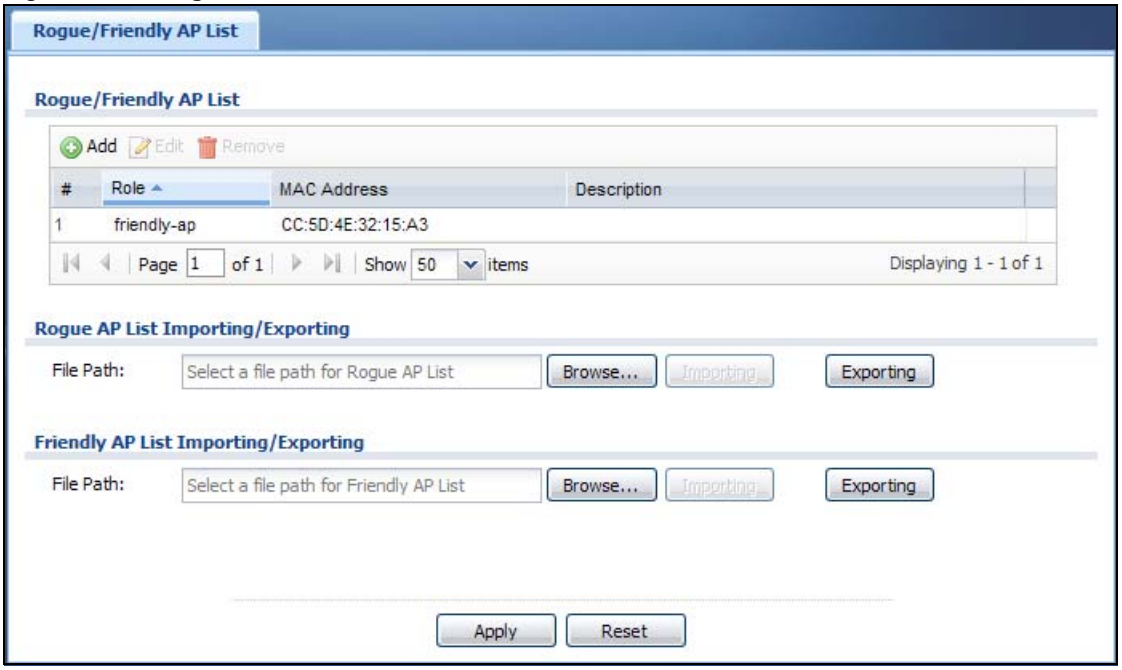
LABEL	DESCRIPTION
Model	This field displays the NWA's model name.
Radio 1 Activate	Select the check box to enable the NWA's first (default) radio.
Radio 1 OP Mode	Select the operating mode for radio 1. **AP Mode** means the radio can receive connections from wireless clients and pass their data traffic through to the NWA to be managed (or subsequently passed on to an upstream gateway for managing). **MON Mode** means the radio monitors the broadcast area for other APs, then passes their information on to the NWA where it can be determined if those APs are friendly or rogue. If a radio is set to this mode it cannot receive connections from wireless clients.
Radio 1 Profile	Select the profile the radio uses. Note: You can only apply a 2.4G AP profile to radio 1. Otherwise, the first radio will not be working.
Radio 2 Activate	This displays if the NWA has a second radio. Select the check box to enable the NWA's second radio.
Radio 2 OP Mode	This displays if the NWA has a second radio. Select the operating mode for radio 2. **AP Mode** means the radio can receive connections from wireless clients and pass their data traffic through to the NWA to be managed (or subsequently passed on to an upstream gateway for managing). **MON Mode** means the radio monitors the broadcast area for other APs, then passes their information on to the NWA where it can be determined if those APs are friendly or rogue. If a radio is set to this mode it cannot receive connections from wireless clients.
Radio 2 Profile	This displays if the NWA has a second radio. Select the profile the radio uses. Note: You can only apply a 5G AP profile to radio 2. Otherwise, the second radio will not be working.
Apply	Click **Apply** to save your changes back to the NWA.
Reset	Click **Reset** to return the screen to its last-saved settings.

6.3 MON Mode

Use this screen to assign APs either to the rogue AP list or the friendly AP list. A rogue AP is a wireless access point operating in a network's coverage area that is not under the control of the network administrator, and which can potentially open up holes in a network's security.

Click **Configuration > Wireless > MON Mode** to access this screen.

Figure 27 Configuration > Wireless > MON Mode



Each field is described in the following table.

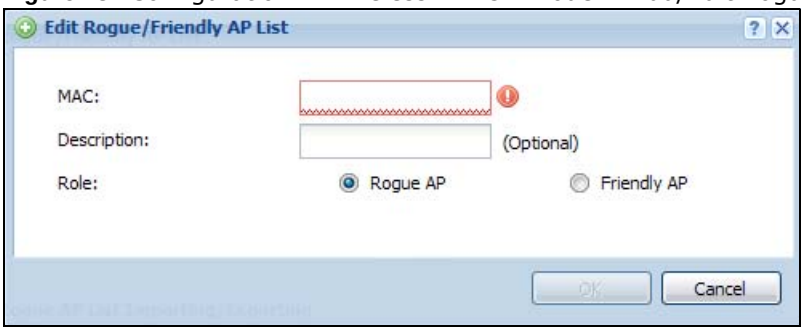
Table 25 Configuration > Wireless > MON Mode

LABEL	DESCRIPTION
Rogue/Friendly AP List	
Add	Click this button to add an AP to the list and assign it either friendly or rogue status.
Edit	Select an AP in the list to edit and reassign its status.
Remove	Select an AP in the list to remove.
#	This field is a sequential value, and it is not associated with any interface.
Role	This field indicates whether the selected AP is a **rogue-ap** or a **friendly-ap**. To change the AP's role, click the **Edit** button.
MAC Address	This field indicates the AP's radio MAC address.
Description	This field displays the AP's description. You can modify this by clicking the **Edit** button.
Importing/Exporting	These controls allow you to export the current list of rogue and friendly APs or import existing lists.
File Path / Browse / Importing	Enter the file name and path of the list you want to import or click the **Browse** button to locate it. Once the **File Path** field has been populated, click **Importing** to bring the list into the NWA. You need to wait a while for the importing process to finish.
Exporting	Click this button to export the current list of either rogue APs or friendly APS.
Apply	Click **Apply** to save your changes back to the NWA.
Reset	Click **Reset** to return the screen to its last-saved settings.

6.3.1 Add/Edit Rogue/Friendly List

Click **Add** or select an AP and click the **Edit** button in the **Configuration > Wireless > MON Mode** table to display this screen.

Figure 28 Configuration > Wireless > MON Mode > Add/Edit Rogue/Friendly AP List



Each field is described in the following table.

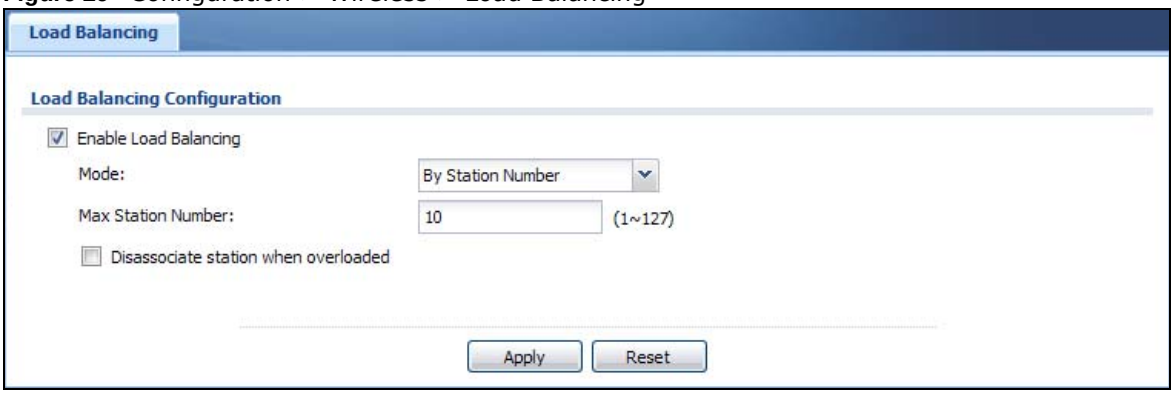
Table 26 Configuration > Wireless > MON Mode > Add/Edit Rogue/Friendly AP List

LABEL	DESCRIPTION
MAC	Enter the MAC address of the AP you want to add to the list. A MAC address is a unique hardware identifier in the following hexadecimal format: xx:xx:xx:xx:xx:xx where xx is a hexadecimal number separated by colons.
Description	Enter up to 60 characters for the AP's description. Spaces and underscores are allowed.
Role	Select either **Rogue AP** or **Friendly AP** for the AP's role.
OK	Click **OK** to save your changes back to the NWA.
Cancel	Click **Cancel** to close the window with changes unsaved.

6.4 Load Balancing

Use this screen to configure wireless network traffic load balancing between the APs on your network. Click **Configuration > Wireless > Load Balancing** to access this screen.

Figure 29 Configuration > Wireless > Load Balancing



Each field is described in the following table.

Table 27 Configuration > Wireless > Load Balancing

LABEL	DESCRIPTION
Enable Load Balancing	Select this to enable load balancing on the NWA.
Mode	Select a mode by which load balancing is carried out. Select **By Station Number** to balance network traffic based on the number of specified stations connect to an AP. Select **By Traffic Level** to balance network traffic based on the volume generated by the stations connected to an AP. Once the threshold is crossed (either the maximum station numbers or with network traffic), then the AP delays association request and authentication request packets from any new station that attempts to make a connection. This allows the station to automatically attempt to connect to another, less burdened AP if one is available.
Max Station Number	Enter the threshold number of stations at which an AP begins load balancing its connections.
Traffic Level	Select the threshold traffic level at which the AP begins load balancing its connections (**Low**, **Medium**, **High**).
Disassociate station when overloaded	Select this option to disassociate wireless clients connected to the AP when it becomes overloaded. If you do not enable this option, then the AP simply delays the connection until it can afford the bandwidth it requires, or it transfers the connection to another AP within its broadcast radius. The disassociation priority is determined automatically by the NWA and is as follows: • **Idle Timeout** - Devices that have been idle the longest will be kicked first. If none of the connected devices are idle, then the priority shifts to **Signal Strength**. • **Signal Strength** - Devices with the weakest signal strength will be kicked first. Note: If you enable this function, you should ensure that there are multiple APs within the broadcast radius that can accept any rejected or kicked wireless clients; otherwise, a wireless client attempting to connect to an overloaded AP will be disassociated permanently and never be allowed to connect.
Apply	Click **Apply** to save your changes back to the NWA.
Reset	Click **Reset** to return the screen to its last-saved settings.

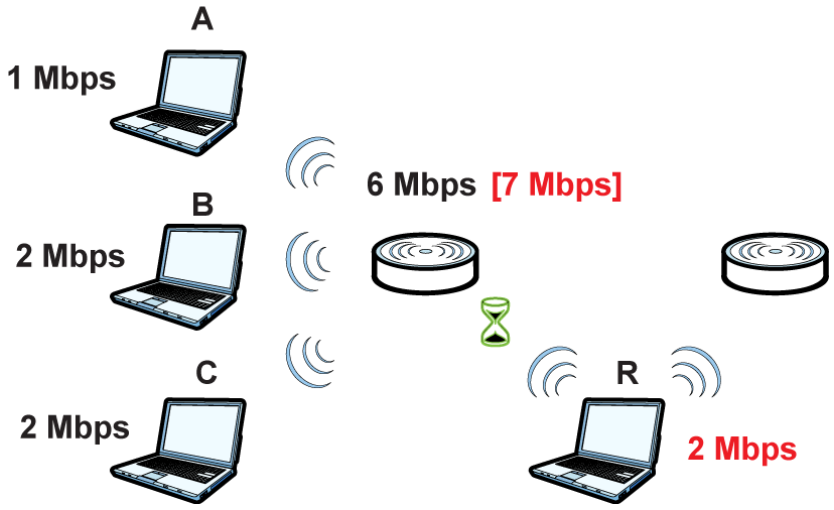
6.4.1 Disassociating and Delaying Connections

When your AP becomes overloaded, there are two basic responses it can take. The first one is to "delay" a client connection. This means that the AP withholds the connection until the data transfer throughput is lowered or the client connection is picked up by another AP. If the client is picked up by another AP then the original AP cannot resume the connection.

For example, here the AP has a balanced bandwidth allotment of 6 Mbps. If laptop **R** connects and it pushes the AP over its allotment, say to 7 Mbps, then the AP delays the red laptop's connection

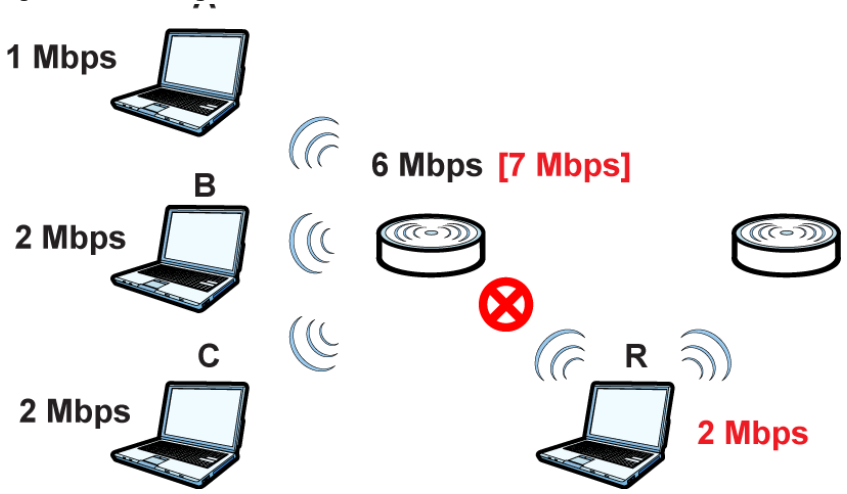
until it can afford the bandwidth or the laptop is picked up by a different AP with bandwidth to spare.

Figure 30 Delaying a Connection



The second response your AP can take is to kick the connections that are pushing it over its balanced bandwidth allotment.

Figure 31 Kicking a Connection

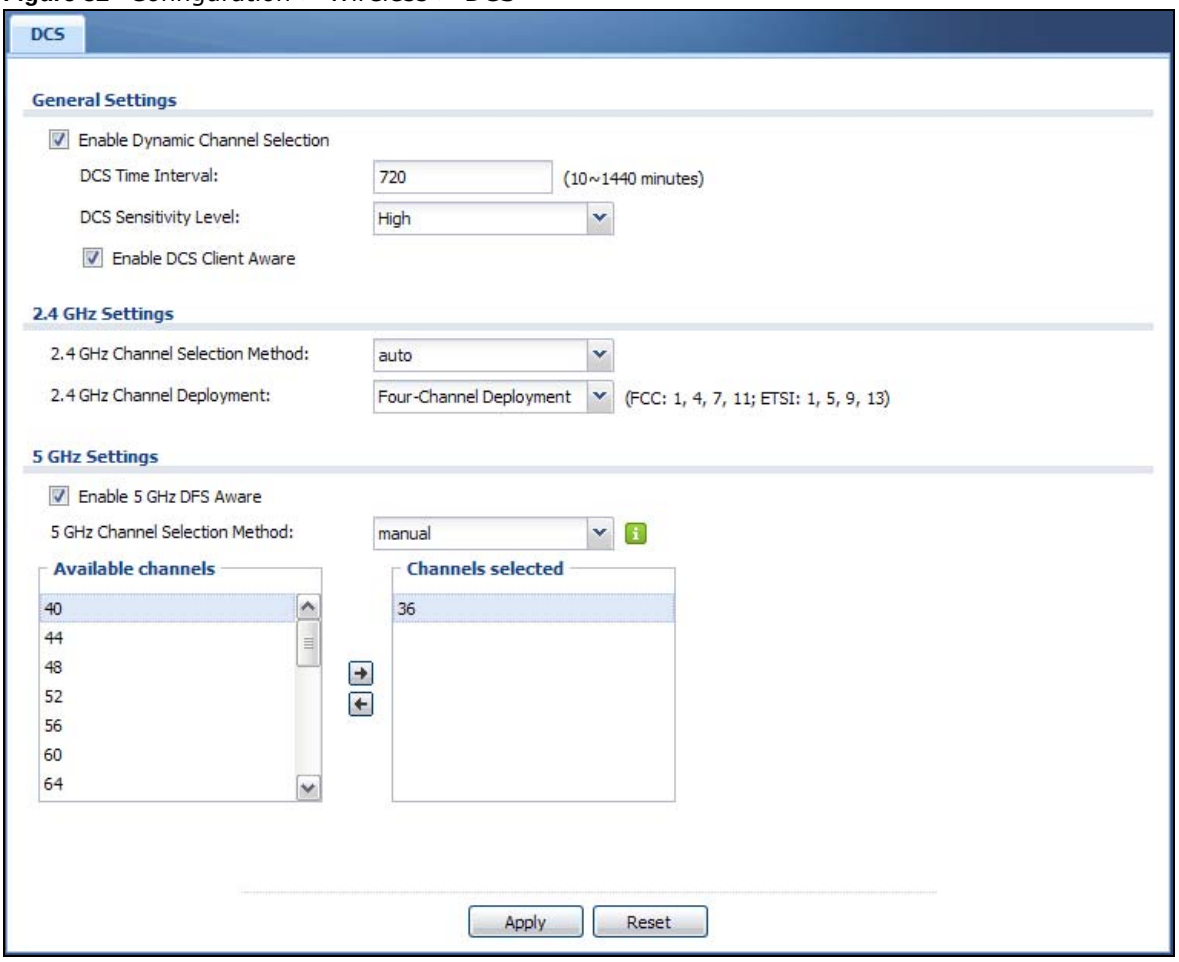


Connections are kicked based on either **idle timeout** or **signal strength**. The NWA first looks to see which devices have been idle the longest, then starts kicking them in order of highest idle time. If no connections are idle, the next criteria the NWA analyzes is signal strength. Devices with the weakest signal strength are kicked first.

6.5 DCS

Use this screen to configure dynamic radio channel selection. Click **Configuration > Wireless > DCS** to access this screen.

Figure 32 Configuration > Wireless > DCS



Each field is described in the following table.

Table 28 Configuration > Wireless > DCS

LABEL	DESCRIPTION
Enable Dynamic Channel Selection	Select this to have the NWA automatically select the radio channel upon which it broadcasts by scanning the area around it and determining what channels are currently being used by other devices.
DCS Time Interval	Enter a number of minutes. This regulates how often the NWA surveys the other APs within its broadcast radius. If the channel on which it is currently broadcasting suddenly comes into use by another AP, the NWA will then dynamically select the next available clean channel or a channel with lower interference.

Table 28 Configuration > Wireless > DCS (continued)

LABEL	DESCRIPTION
DCS Sensitivity Level	Select the AP's sensitivity level toward other channels. Options are **High**, **Medium**, and **Low**. Generally, as long as the area in which your AP is located has minimal interference from other devices you can set the **DCS Sensitivity Level** to **Low**. This means that the AP has a very broad tolerance. If you are not sure about the number and location of any other devices in the region, set the level to **Medium**. The AP's tolerance for interference is relatively narrow. On the other hand, if you know there are numerous other devices in the region, you should set the level to **High** to keep the interference to a minimum. In this case, the NWA's tolerance for interference is quite strict. Note: Generally speaking, the higher the sensitivity level, the more frequently the AP switches channels. As a consequence, anyone connected to the AP will experience more frequent disconnects and reconnects unless you select **Enable DCS Client Aware**.
Enable DCS Client Aware	Select this to have the AP wait until all connected clients have disconnected before switching channels. If you disable this then the AP switches channels immediately regardless of any client connections. In this instance, clients that are connected to the AP when it switches channels are dropped.
2.4 GHz Channel Selection Method	Select how you want to specify the channels the NWA switches between for 2.4 GHz operation. Select **auto** to have the NWA display a **2.4 GHz Channel Deployment** field you can use to limit channel switching to 3 or 4 channels. Select **manual** to select the individual channels the NWA switches between. Select channels from the **Available channels** list and use the right arrow button to move them to the **Channels selected** list.
2.4 GHz Channel Deployment	This is available when the **2.4 GHz Channel Selection Method** is set to **auto**. Select **Three-Channel Deployment** to limit channel switching to channels 1,6, and 11, the three channels that are sufficiently attenuated to have almost no impact on one another. In other words, this allows you to minimize channel interference by limiting channel-hopping to these three "safe" channels. Select **Four-Channel Deployment** to limit channel switching to four channels. Depending on the country domain, if the only allowable channels are 1-11 then the NWA uses channels 1, 4, 7, 11 in this configuration; otherwise, the NWA uses channels 1, 5, 9, 13 in this configuration. Four channel deployment expands your pool of possible channels while keeping the channel interference to a minimum.
Enable 5 GHz DFS Aware	Select this if your APs are operating in an area known to have RADAR devices. This allows the device to downgrade its frequency to below 5 GHz in the event a RADAR signal is detected, thus preventing it from interfering with that signal. Enabling this forces the AP to select a non-DFS channel.
5 GHz Channel Selection Method	Select how you want to specify the channels the NWA switches between for 5 GHz operation. Select **auto** to have the NWA automatically select the best channel. Select **manual** to select the individual channels the NWA switches between. Select channels from the **Available channels** list and use the right arrow button to move them to the **Channels selected** list.
Apply	Click **Apply** to save your changes back to the NWA.
Reset	Click **Reset** to return the screen to its last-saved settings.

6.6 Technical Reference

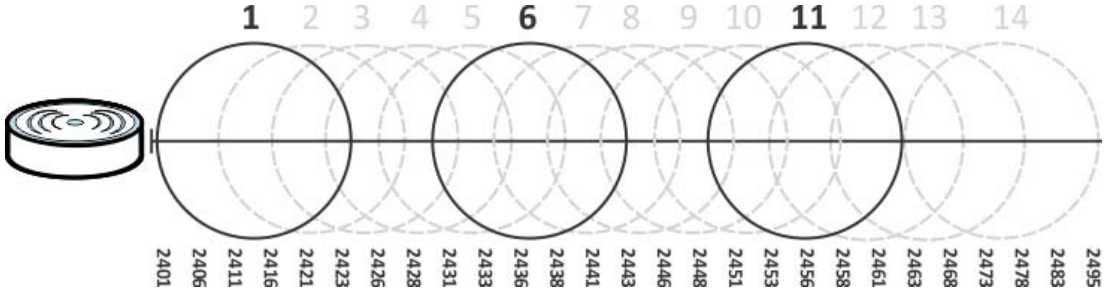
The following section contains additional technical information about the features described in this chapter.

Dynamic Channel Selection

When numerous APs broadcast within a given area, they introduce the possibility of heightened radio interference, especially if some or all of them are broadcasting on the same radio channel. If the interference becomes too great, then the network administrator must open his AP configuration options and manually change the channel to one that no other AP is using (or at least a channel that has a lower level of interference) in order to give the connected stations a minimum degree of interference. Dynamic channel selection frees the network administrator from this task by letting the AP do it automatically. The AP can scan the area around it looking for the channel with the least amount of interference.

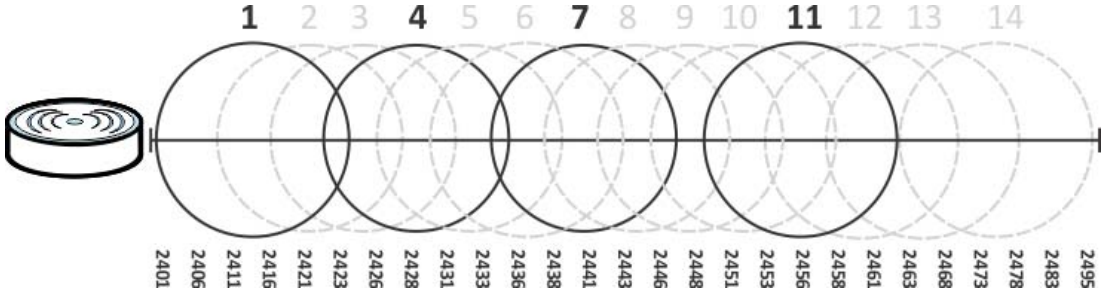
In the 2.4 GHz spectrum, each channel from 1 to 13 is broken up into discrete 22 MHz segments that are spaced 5 MHz apart. Channel 1 is centered on 2.412 GHz while channel 13 is centered on 2.472 GHz.

Figure 33 An Example Three-Channel Deployment



Three channels are situated in such a way as to create almost no interference with one another if used exclusively: 1, 6 and 11. When an AP broadcasts on any of these three channels, it should not interfere with neighboring APs as long as they are also limited to same trio.

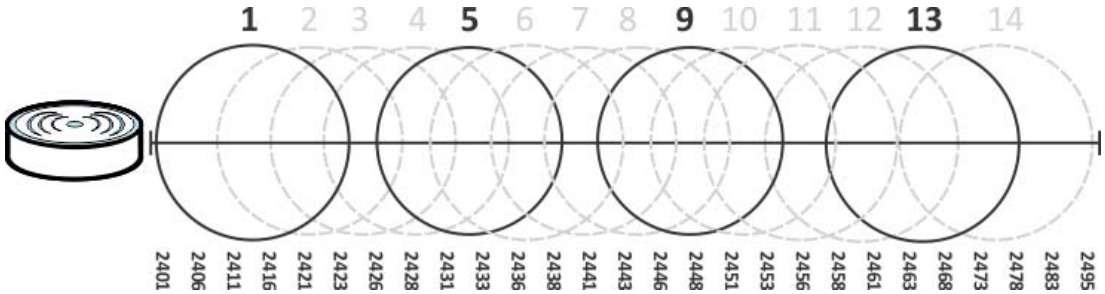
Figure 34 An Example Four-Channel Deployment



However, some regions require the use of other channels and often use a safety scheme with the following four channels: 1, 4, 7 and 11. While they are situated sufficiently close to both each other and the three so-called "safe" channels (1,6 and 11) that interference becomes inevitable, the severity of it is dependent upon other factors: proximity to the affected AP, signal strength, activity, and so on.

Finally, there is an alternative four channel scheme for ETSI, consisting of channels 1, 5, 9, 13. This offers significantly less overlap that the other one.

Figure 35 An Alternative Four-Channel Deployment



Load Balancing

Because there is a hard upper limit on an AP's wireless bandwidth, load balancing can be crucial in areas crowded with wireless users. Rather than let every user connect and subsequently dilute the available bandwidth to the point where each connecting device receives a meager trickle, the load balanced AP instead limits the incoming connections as a means to maintain bandwidth integrity.

There are two kinds of wireless load balancing available on the NWA:

Load balancing by station number limits the number of devices allowed to connect to your AP. If you know exactly how many stations you want to let connect, choose this option.

For example, if your company's graphic design team has their own AP and they have 10 computers, you can load balance for 10. Later, if someone from the sales department visits the graphic design team's offices for a meeting and he tries to access the network, his computer's connection is delayed, giving it the opportunity to connect to a different, neighboring AP. If he still connects to the AP regardless of the delay, then the AP may boot other people who are already connected in order to associate with the new connection.

Load balancing by traffic level limits the number of connections to the AP based on maximum bandwidth available. If you are uncertain as to the exact number of wireless connections you will have then choose this option. By setting a maximum bandwidth cap, you allow any number of devices to connect as long as their total bandwidth usage does not exceed the configured bandwidth cap associated with this setting. Once the cap is hit, any new connections are rejected or delayed provided that there are other APs in range.

Imagine a coffee shop in a crowded business district that offers free wireless connectivity to its customers. The coffee shop owner can't possibly know how many connections his AP will have at any given moment. As such, he decides to put a limit on the bandwidth that is available to his customers but not on the actual number of connections he allows. This means anyone can connect to his wireless network as long as the AP has the bandwidth to spare. If too many people connect and the AP hits its bandwidth cap then all new connections must basically wait for their turn or get shunted to the nearest identical AP.

7

User

7.1 Overview

This chapter describes how to set up user accounts and user settings for the NWA.

7.1.1 What You Can Do in this Chapter

- The **User** screen (see Section 7.2 on page 66) provides a summary of all user accounts.
- The **Setting** screen (see Section 7.3 on page 68) controls default settings, login settings, lockout settings, and other user settings for the NWA.

7.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

User Account

A user account defines the privileges of a user logged into the NWA. User accounts are used in controlling access to configuration and services in the NWA.

User Types

These are the types of user accounts the NWA uses.

Table 29 Types of User Accounts

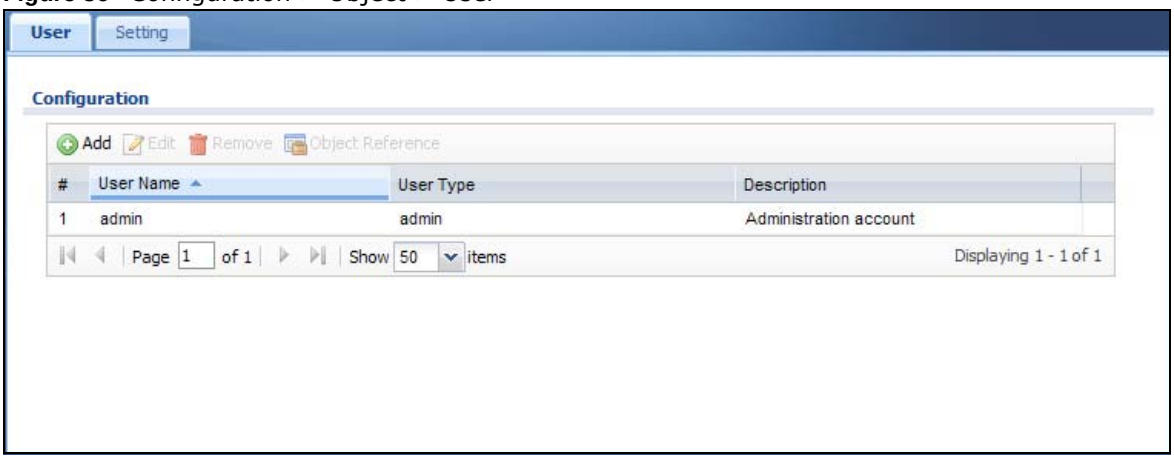
TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
admin	Change NWA configuration (web, CLI)	WWW, TELNET, SSH, FTP
limited-admin	Look at NWA configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH
Access Users		
user	Used for the embedded RADIUS server and SNMPv3 user access Browse user-mode commands (CLI)	

Note: The default **admin** account is always authenticated locally, regardless of the authentication method setting.

7.2 User Summary

The **User** screen provides a summary of all user accounts. To access this screen click **Configuration > Object > User**.

Figure 36 Configuration > Object > User



The following table describes the labels in this screen.

Table 30 Configuration > Object > User

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The NWA confirms you want to remove it before doing so.
Object Reference	Select an entry and click **Object Reference** to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific user.
User Name	This field displays the user name of each user.
User Type	This field displays type of user this account was configured as. • **admin** - this user can look at and change the configuration of the NWA • **limited-admin** - this user can look at the configuration of the NWA but not to change it • **user** - this user has access to the NWA's services but cannot look at the configuration
Description	This field displays the description for each user.

7.2.1 Add/Edit User

The **User Add/Edit** screen allows you to create a new user account or edit an existing one.

7.2.1.1 Rules for User Names

Enter a user name from 1 to 31 characters.

The user name can only contain the following characters:

- Alphanumeric A-z 0-9 (there is no unicode support)
- _ [underscores]
- - [dashes]

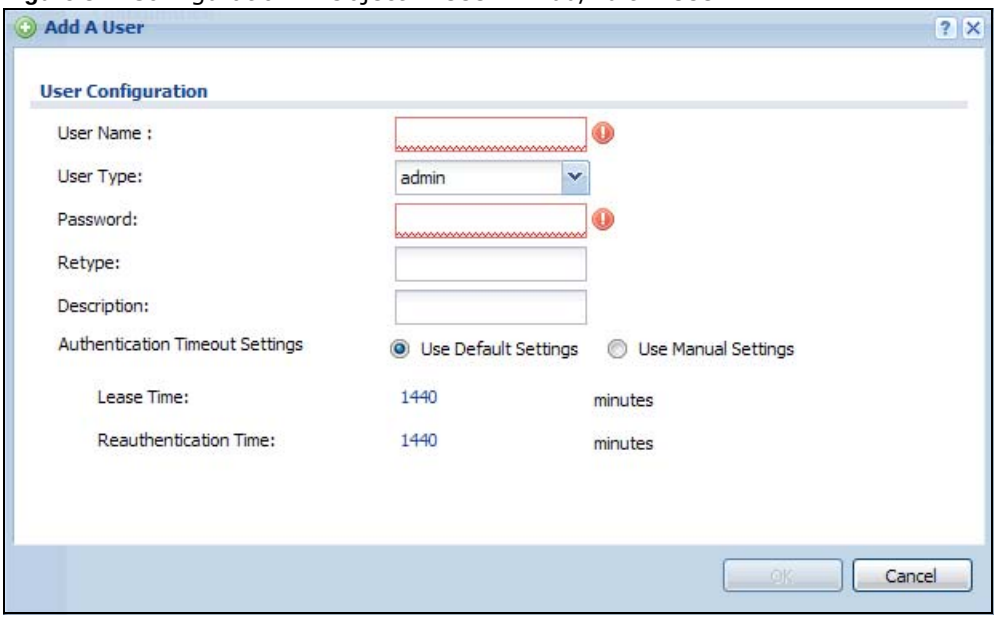
The first character must be alphabetical (A-Z a-z), an underscore (_), or a dash (-). Other limitations on user names are:

- User names are case-sensitive. If you enter a user 'bob' but use 'BOB' when connecting via CIFS or FTP, it will use the account settings used for 'BOB' not 'bob'.
- User names have to be different than user group names.
- Here are the reserved user names:

• adm	• admin	• any	• bin	• daemon
• debug	• devicehaecived	• ftp	• games	• halt
• ldap-users	• lp	• mail	• news	• nobody
• operator	• radius-users	• root	• shutdown	• sshd
• sync	• uucp	• zyxel		

To access this screen, go to the **User** screen, and click **Add** or **Edit**.

Figure 37 Configuration > Object > User > Add/Edit A User



The following table describes the labels in this screen.

Table 31 Configuration > User > User > Add/Edit A User

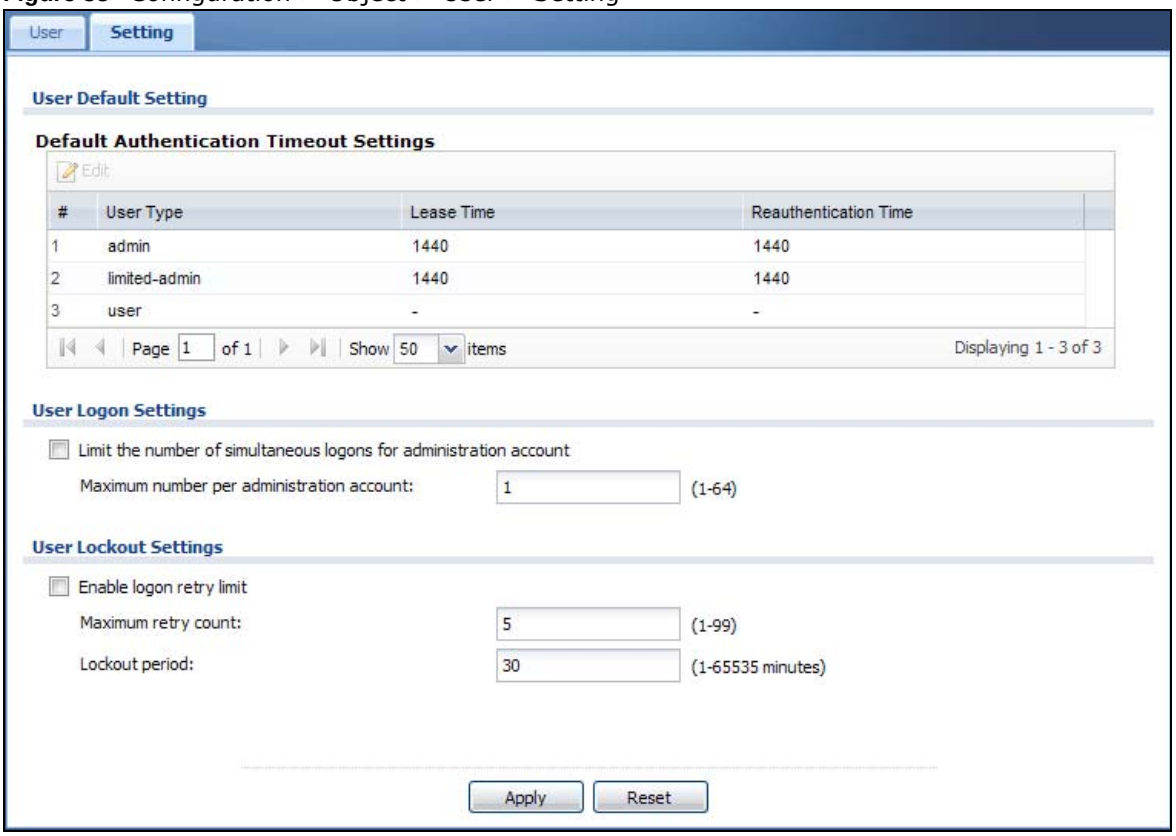
LABEL	DESCRIPTION
User Name	Type the user name for this user account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User names have to be different than user group names, and some words are reserved.
User Type	Select what type of user this is. Choices are: • **admin** - this user can look at and change the configuration of the NWA • **limited-admin** - this user can look at the configuration of the NWA but not to change it • **user** - this is used for embedded RADIUS server and SNMPv3 user access
Password	This field is not available if you select the **ext-user** or **ext-group-user** type. Enter the password of this user account. It can consist of 4 - 31 alphanumeric characters.
Retype	Re-enter the password to make sure you have entered it correctly.
Description	Enter the description of each user, if any. You can use up to 60 printable ASCII characters. Default descriptions are provided.
Authentication Timeout Settings	This field is not available if the user type is **user**. If you want to set authentication timeout to a value other than the default settings, select **Use Manual Settings** then fill your preferred values in the fields that follow.
Lease Time	This field is not available if the user type is **user**. Enter the number of minutes this user has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator.
Reauthentication Time	This field is not available if the user type is **user**. Type the number of minutes this user can be logged into the NWA in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out.
OK	Click **OK** to save your changes back to the NWA.
Cancel	Click **Cancel** to exit this screen without saving your changes.

7.3 Setting

This screen controls default settings, login settings, lockout settings, and other user settings for the NWA.

To access this screen, login to the Web Configurator, and click **Configuration > Object > User > Setting**.

Figure 38 Configuration > Object > User > Setting


User
Setting
User Default Setting
Default Authentication Timeout Settings
Edit
User Type Lease Time Reauthentication Time
1 admin 1440 1440
2 limited-admin 1440 1440
3 user - -
Page 1 of 1 Show 50 items
Displaying 1 - 3 of 3
User Logon Settings
Limit the number of simultaneous logons for administration account
Maximum number per administration account: 1 (1-64)
User Lockout Settings
Enable logon retry limit
Maximum retry count: 5 (1-99)
Lockout period: 30 (1-65535 minutes)
Apply
Reset

The following table describes the labels in this screen.

Table 32 Configuration > Object > User > Setting

LABEL	DESCRIPTION
User Default Setting	
Default Authentication Timeout Settings	These authentication timeout settings are used by default when you create a new user account. They also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
#	This field is a sequential value, and it is not associated with a specific entry.
User Type	These are the kinds of user account the NWA supports. • **admin** - this user can look at and change the configuration of the NWA • **limited-admin** - this user can look at the configuration of the NWA but not to change it • **user** - this is used for embedded RADIUS server and SNMPv3 user access
Lease Time	This is the default lease time in minutes for each type of user account. It defines the number of minutes the user has to renew the current session before the user is logged out. Admin users renew the session every time the main screen refreshes in the Web Configurator.

Table 32 Configuration > Object > User > Setting (continued)

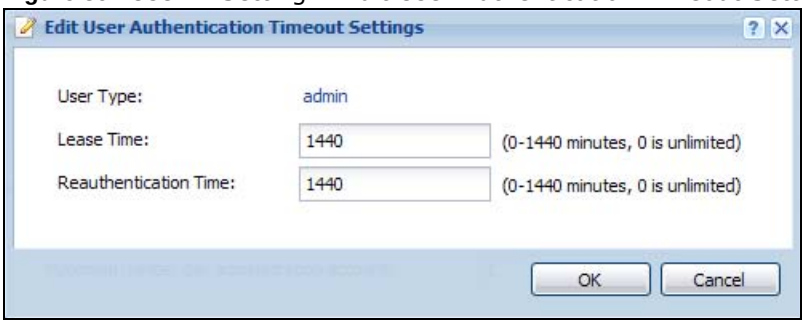
LABEL	DESCRIPTION
Reauthentication Time	This is the default reauthentication time in minutes for each type of user account. It defines the number of minutes the user can be logged into the NWA in one session before having to log in again. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out.
User Logon Settings	
Limit the number of simultaneous logons for administration account	Select this check box if you want to set a limit on the number of simultaneous logins by admin users. If you do not select this, admin users can login as many times as they want at the same time using the same or different IP addresses.
Maximum number per administration account	This field is effective when **Limit ... for administration account** is checked. Type the maximum number of simultaneous logins by each admin user.
User Lockout Settings	
Enable logon retry limit	Select this check box to set a limit on the number of times each user can login unsuccessfully (for example, wrong password) before the IP address is locked out for a specified amount of time.
Maximum retry count	This field is effective when **Enable logon retry limit** is checked. Type the maximum number of times each user can login unsuccessfully before the IP address is locked out for the specified **lockout period**. The number must be between 1 and 99.
Lockout period	This field is effective when **Enable logon retry limit** is checked. Type the number of minutes the user must wait to try to login again, if **logon retry limit** is enabled and the **maximum retry count** is reached. This number must be between 1 and 65,535 (about 45.5 days).
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to return the screen to its last-saved settings.

7.3.1 Edit User Authentication Timeout Settings

This screen allows you to set the default authentication timeout settings for the selected type of user account. These default authentication timeout settings also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.

To access this screen, go to the **Configuration > Object > User > Setting** screen, select one of the **Default Authentication Timeout Settings** entry and click the **Edit** icon.

Figure 39 User > Setting > Edit User Authentication Timeout Settings



The following table describes the labels in this screen.

Table 33 User > Setting > Edit User Authentication Timeout Settings

LABEL	DESCRIPTION
User Type	This read-only field identifies the type of user account for which you are configuring the default settings. • **admin** - this user can look at and change the configuration of the NWA. • **limited-admin** - this user can look at the configuration of the NWA but not to change it.
Lease Time	Enter the number of minutes this type of user account has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the **Renew** button on their screen. If you allow access users to renew time automatically, the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	Type the number of minutes this type of user account can be logged into the NWA in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out.
OK	Click **OK** to save your changes back to the NWA.
Cancel	Click **Cancel** to exit this screen without saving your changes.

8

AP Profile

8.1 Overview

This chapter shows you how to configure preset profiles for the NWA.

8.1.1 What You Can Do in this Chapter

- The **Radio** screen (Section 8.2 on page 74) creates radio configurations that can be used by the APs.
- The **SSID** screen (Section 8.3 on page 79) configures three different types of profiles for your networked APs.

8.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Wireless Profiles

At the heart of all wireless AP configurations on the NWA are profiles. A profile represents a group of saved settings that you can use across any number of connected APs. You can set up the following wireless profile types:

- **Radio** - This profile type defines the properties of an AP's radio transmitter. You can have a maximum of 32 radio profiles on the NWA.
- **SSID** - This profile type defines the properties of a single wireless network signal broadcast by an AP. Each radio on a single AP can broadcast up to 8 SSIDs. You can have a maximum of 32 SSID profiles on the NWA.
- **Security** - This profile type defines the security settings used by a single SSID. It controls the encryption method required for a wireless client to associate itself with the SSID. You can have a maximum of 32 security profiles on the NWA.
- **MAC Filtering** - This profile provides an additional layer of security for an SSID, allowing you to block access or allow access to that SSID based on wireless client MAC addresses. If a client's MAC address is on the list, then it is either allowed or denied, depending on how you set up the MAC Filter profile. You can have a maximum of 32 MAC filtering profiles on the NWA.
- **Layer-2 Isolation** - This profile defines the MAC addresses of the devices that you want to allow the associated wireless clients to have access to when layer-2 isolation is enabled.

SSID

The SSID (Service Set IDentifier) is the name that identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. In other words, it is the name of the wireless network that clients use to connect to it.

WEP

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the AP and the wireless stations associated with it in order to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. Key differences between WPA(2) and WEP are improved data encryption and user authentication.

IEEE 802.1x

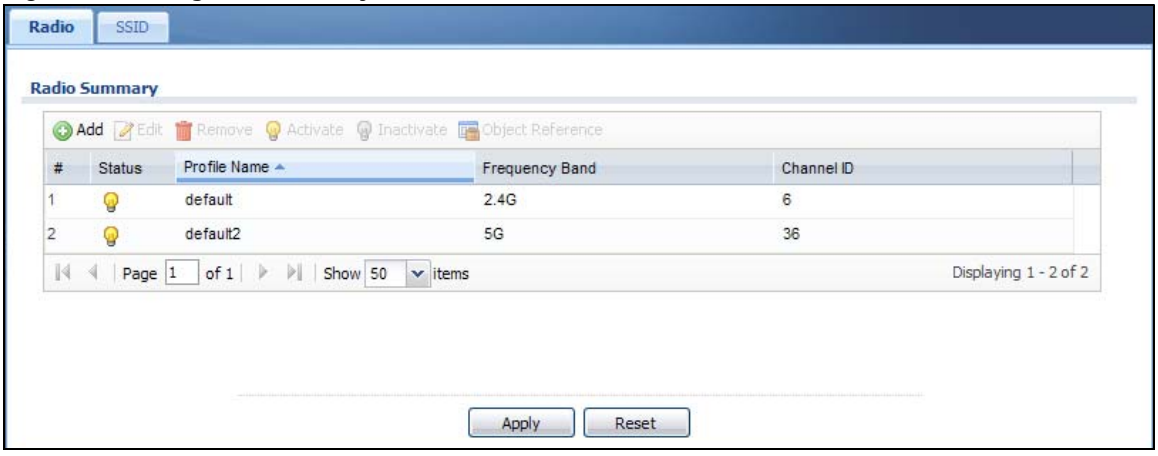
The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication is done using an external RADIUS server.

8.2 Radio

This screen allows you to create radio profiles for the NWA. A radio profile is a list of settings that an NWA can use to configure its radio transmitter(s). To access this screen click **Configuration > Object > AP Profile**.

Note: You can have a maximum of 32 radio profiles on the NWA.

Figure 40 Configuration > Object > AP Profile > Radio



The following table describes the labels in this screen.

Table 34 Configuration > Object > AP Profile > Radio

LABEL	DESCRIPTION
Add	Click this to add a new radio profile.
Edit	Click this to edit the selected radio profile.

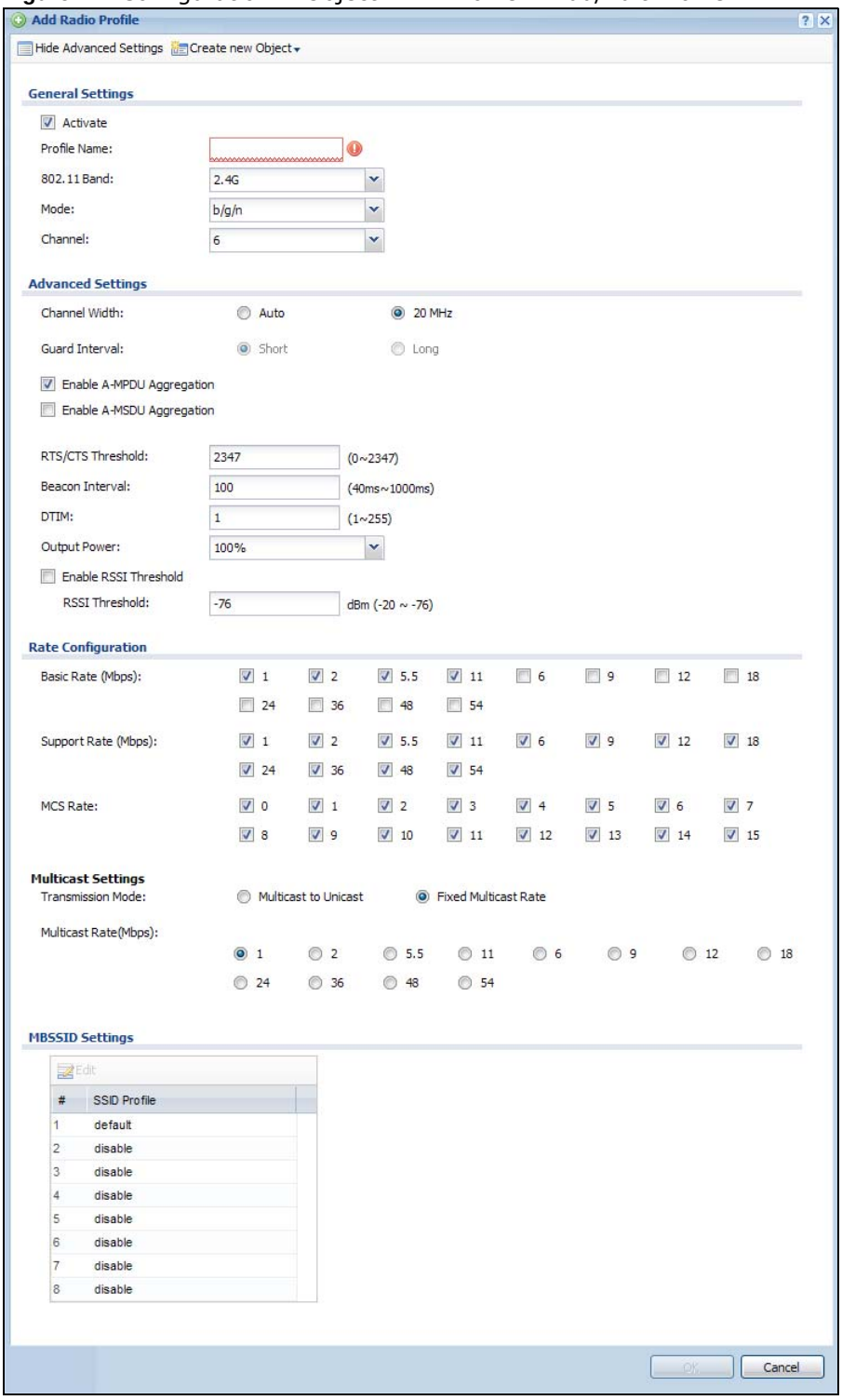
Table 34 Configuration > Object > AP Profile > Radio (continued)

LABEL	DESCRIPTION
Remove	Click this to remove the selected radio profile.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Object Reference	Click this to view which other objects are linked to the selected radio profile.
#	This field is a sequential value, and it is not associated with a specific user.
Status	This field shows whether or not the entry is activated.
Profile Name	This field indicates the name assigned to the radio profile.
Frequency Band	This field indicates the frequency band which this radio profile is configured to use.
Channel ID	This field indicates the broadcast channel which this radio profile is configured to use.

8.2.1 Add/Edit Radio Profile

This screen allows you to create a new radio profile or edit an existing one. To access this screen, click the **Add** button or select a radio profile from the list and click the **Edit** button.

Figure 41 Configuration > Object > AP Profile > Add/Edit Profile



The following table describes the labels in this screen.

Table 35 Configuration > Object > AP Profile > Add/Edit Profile

LABEL	DESCRIPTION
Hide / Show Advanced Settings	Click this to hide or show the **Advanced Settings** in this window.
Create New Object	Select an item from this menu to create a new object of that type. Any objects created in this way are automatically linked to this radio profile.
General Settings	
Activate	Select this option to make this profile active.
Profile Name	Enter up to 31 alphanumeric characters to be used as this profile's name. Spaces and underscores are allowed.
802.11 Band	Select the wireless band which this radio profile should use. Not all NWAs support both 2.4 GHz and 5 GHz frequency bands. 2.4 GHz is the frequency used by IEEE 802.11b/g/n wireless clients. 5 GHz is the frequency used by IEEE 802.11a/n wireless clients.
Mode	If you set **802.11 Band** to **2.4G**, you can select from the following: • **b/g**: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the NWA. The NWA adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices. • **b/g/n**: allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the NWA. The transmission rate of your NWA might be reduced. If you set **802.11 Band** to **5G**, you can select from the following: • **a**: allows only IEEE 802.11a compliant WLAN devices to associate with the NWA. • **a/n**: allows both IEEE802.11n and IEEE802.11a compliant WLAN devices to associate with the NWA. The transmission rate of your NWA might be reduced.
Channel	Select the wireless channel which this radio profile should use. It is recommended that you choose the channel least in use by other APs in the region where this profile will be implemented. This will reduce the amount of interference between wireless clients and the AP to which this profile is assigned.
Advanced Settings	
Channel Width	Select the channel bandwidth you want to use for your wireless network. Select **Auto** to allow the NWA to adjust the channel bandwidth depending on network conditions. Select **20 MHz** if you want to lessen radio interference with other wireless devices in your neighborhood.
Guard Interval	Set the guard interval for this radio profile to either **short** or **long**. The guard interval is the gap introduced between data transmission from users in order to reduce interference. Reducing the interval increases data transfer rates but also increases interference. Increasing the interval reduces data transfer rates but also reduces interference.
Enable A-MPDU Aggregation	Select this to enable A-MPDU aggregation. Message Protocol Data Unit (MPDU) aggregation collects Ethernet frames along with their 802.11n headers and wraps them in a 802.11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates.

Table 35 Configuration > Object > AP Profile > Add/Edit Profile (continued)

LABEL	DESCRIPTION
Enable A-MSDU Aggregation	Select this to enable A-MSDU aggregation. Mac Service Data Unit (MSDU) aggregation collects Ethernet frames without any of their 802.11n headers and wraps the header-less payload in a single 802.11n MAC header. This method is useful for increasing bandwidth throughput. It is also more efficient than A-MPDU except in environments that are prone to high error rates.
Disable-Channel Switch for DFS	This field is available only if you set **802.11 Band** to **5G**. DFS (dynamic frequency selection) allows an AP to detect other devices in the same channel. If there is another device using the same channel, the AP changes to a different channel, so that it can avoid interference with radar systems or other wireless networks. Select this option to disable DFS on this radio.
RTS/CTS Threshold	Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions). A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. A high value helps save current consumption of the access point.
DTIM	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.
Output Power	Set the output power of the AP in this field. If there is a high density of APs in an area, decrease the output power of the NWA5160N to reduce interference with other APs. Select one of the following **100%(Full Power)**, **50%**, **25%**, or **12.5%**. See the product specifications for more information on your NWA's output power. Note: Reducing the output power also reduces the NWA's effective broadcast radius.
Enable RSSI Threshold	Use the Received Signal Strength Indication (RSSI) threshold to ensure wireless clients receive good throughput. This allows only wireless clients with a strong signal to connect to the AP. Select the check box and set a minimum client signal strength for connecting to the AP. -20 dBm is the strongest signal you can require and -76 is the weakest. Clear the check box to not require wireless clients to have a minimum signal strength to connect to the AP.
RSSI Threshold	If you enable the RSSI threshold, set a threshold value here.
Rate Configuration	This section controls the data rates permitted for clients. For each rate, select a rate option from its list. The rates are: • **Basic Rate (Mbps)** - Set the basic rate configuration in Mbps. Clients can always connect to the NWA at this speed. • **Support Rate (Mbps)** - Set the support rate configuration in Mbps. Clients can connect to the NWA at this speed, when permitted to do so by the NWA. • **MCS Rate** - Set the MCS rate configuration. EEE 802.11n supports many different data rates which are called MCS rates. MCS stands for Modulation and Coding Scheme. This is an 802.11n feature that increases the wireless network performance in terms of throughput.

Table 35 Configuration > Object > AP Profile > Add/Edit Profile (continued)

LABEL	DESCRIPTION
Multicast Settings	
Transmission Mode	Specify how the NWA handles wireless multicast traffic. Select **Multicast to Unicast** to broadcast wireless multicast traffic to all of the wireless clients as unicast traffic. Unicast traffic dynamically changes the data rate based on the application's bandwidth requirements. The retransmit mechanism of unicast traffic provides more reliable transmission of the multicast traffic, although it also produces duplicate packets. Select **Fixed Multicast Rate** to send multicast traffic to all wireless clients at a single data rate. You must know the multicast application's bandwidth requirements and set it in the following field.
Multicast Rate(Mbps)	If you set **Transmission Mode** to **Fixed Multicast Rate**, select a data rate at which the NWA transmits multicast packets to wireless clients. For example, to deploy 4 Mbps video, select a fixed multicast rate higher than 4 Mbps.
MBSSID Settings	This section displays if you set the **Operating Mode** to **MBSSID**. It allows you to associate an SSID profile with the radio profile.
Edit	Select an SSID and click this button to reassign it. The selected SSID becomes editable immediately upon clicking.
SSID Profile	Indicates which SSID profile is associated with this radio profile.
OK	Click **OK** to save your changes back to the NWA.
Cancel	Click **Cancel** to exit this screen without saving your changes.

8.3 SSID

The SSID screens allow you to configure three different types of profiles for your networked APs: an SSID list, which can assign specific SSID configurations to your APs; a security list, which can assign specific encryption methods to the APs when allowing wireless clients to connect to them; and a MAC filter list, which can limit connections to an AP based on wireless clients MAC addresses.

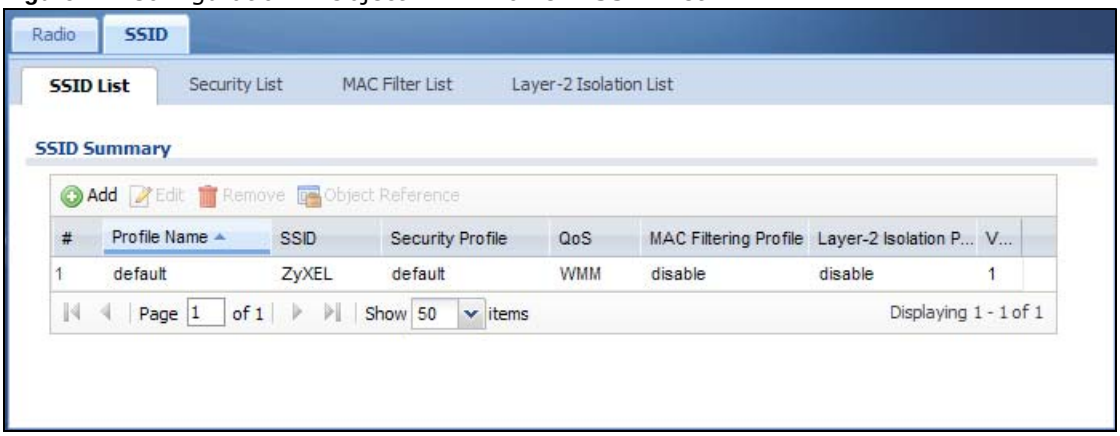
8.3.1 SSID List

This screen allows you to create and manage SSID configurations that can be used by the APs. An SSID, or Service Set IDentifier, is basically the name of the wireless network to which a wireless client can connect. The SSID appears as readable text to any device capable of scanning for wireless frequencies (such as the WiFi adapter in a laptop), and is displayed as the wireless network name when a person makes a connection to it.

To access this screen click **Configuration > Object > AP Profile > SSID**.

Note: You can have a maximum of 32 SSID profiles on the NWA.

Figure 42 Configuration > Object > AP Profile > SSID List



The following table describes the labels in this screen.

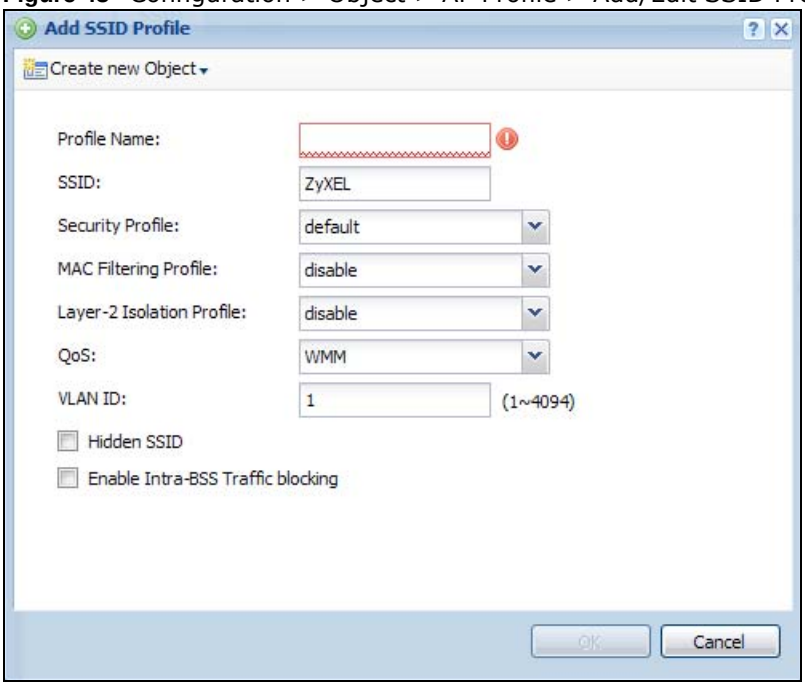
Table 36 Configuration > Object > AP Profile > SSID List

LABEL	DESCRIPTION
Add	Click this to add a new SSID profile.
Edit	Click this to edit the selected SSID profile.
Remove	Click this to remove the selected SSID profile.
Object Reference	Click this to view which other objects are linked to the selected SSID profile (for example, radio profile).
#	This field is a sequential value, and it is not associated with a specific user.
Profile Name	This field indicates the name assigned to the SSID profile.
SSID	This field indicates the SSID name as it appears to wireless clients.
Security Profile	This field indicates which (if any) security profile is associated with the SSID profile.
QOS	This field indicates the QoS type associated with the SSID profile.
MAC Filtering Profile	This field indicates which (if any) MAC filter Profile is associated with the SSID profile.
Layer-2 Isolation Profile	This field indicates which (if any) layer-2 isolation Profile is associated with the SSID profile.
VLAN ID	This field indicates the VLAN ID associated with the SSID profile.

8.3.1.1 Add/Edit SSID Profile

This screen allows you to create a new SSID profile or edit an existing one. To access this screen, click the **Add** button or select an SSID profile from the list and click the **Edit** button.

Figure 43 Configuration > Object > AP Profile > Add/Edit SSID Profile



The following table describes the labels in this screen.

Table 37 Configuration > Object > AP Profile > Add/Edit SSID Profile

LABEL	DESCRIPTION
Create new Object	Select an object type from the list to create a new one associated with this SSID profile.
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
SSID	Enter the SSID name for this profile. This is the name visible on the network to wireless clients. Enter up to 32 characters, spaces and underscores are allowed.
Security Profile	Select a security profile from this list to associate with this SSID. If none exist, you can use the **Create new Object** menu to create one. Note: It is highly recommended that you create security profiles for all of your SSIDs to enhance your network security.
MAC Filtering Profile	Select a MAC filtering profile from the list to associate with this SSID. If none exist, you can sue the **Create new Object** menu to create one. MAC filtering allows you to limit the wireless clients connecting to your network through a particular SSID by wireless client MAC addresses. Any clients that have MAC addresses not in the MAC filtering profile of allowed addresses are denied connections. The **disable** setting means no MAC filtering is used.

Table 37 Configuration > Object > AP Profile > Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
Layer-2 Isolation Profile	Select a layer-2 isolation profile from the list to associate with this SSID. If none exist, you can sue the **Create new Object** menu to create one. Layer-2 isolation allows you to prevent wireless clients associated with your NWA from communicating with other wireless clients, APs, computers or routers in a network. The **disable** setting means no layer-2 isolation is used.
QoS	Select a Quality of Service (QoS) access category to associate with this SSID. Access categories minimize the delay of data packets across a wireless network. Certain categories, such as video or voice, are given a higher priority due to the time sensitive nature of their data packets. QoS access categories are as follows: **disable**: Turns off QoS for this SSID. All data packets are treated equally and not tagged with access categories. **WMM**: Enables automatic tagging of data packets. The NWA assigns access categories to the SSID by examining data as it passes through it and making a best guess effort. If something looks like video traffic, for instance, it is tagged as such. **WMM_VOICE**: All wireless traffic to the SSID is tagged as voice data. This is recommended if an SSID is used for activities like placing and receiving VoIP phone calls. **WMM_VIDEO**: All wireless traffic to the SSID is tagged as video data. This is recommended for activities like video conferencing. **WMM_BEST_EFFORT**: All wireless traffic to the SSID is tagged as "best effort," meaning the data travels the best route it can without displacing higher priority traffic. This is good for activities that do not require the best bandwidth throughput, such as surfing the Internet. **WMM_BACKGROUND**: All wireless traffic to the SSID is tagged as low priority or "background traffic", meaning all other access categories take precedence over this one. If traffic from an SSID does not have strict throughput requirements, then this access category is recommended. For example, an SSID that only has network printers connected to it.
VLAN ID	Enter a VLAN ID for the NWA to use to tag traffic originating from this SSID.
Hidden SSID	Select this if you want to "hide" your SSID from wireless clients. This tells any wireless clients in the vicinity of the AP using this SSID profile not to display its SSID name as a potential connection. Not all wireless clients respect this flag and display it anyway. When an SSID is "hidden" and a wireless client cannot see it, the only way you can connect to the SSID is by manually entering the SSID name in your wireless connection setup screen(s) (these vary by client, client connectivity software, and operating system).
Enable Intra-BSS Traffic Blocking	Select this option to prevent crossover traffic from within the same SSID.
OK	Click **OK** to save your changes back to the NWA.
Cancel	Click **Cancel** to exit this screen without saving your changes.

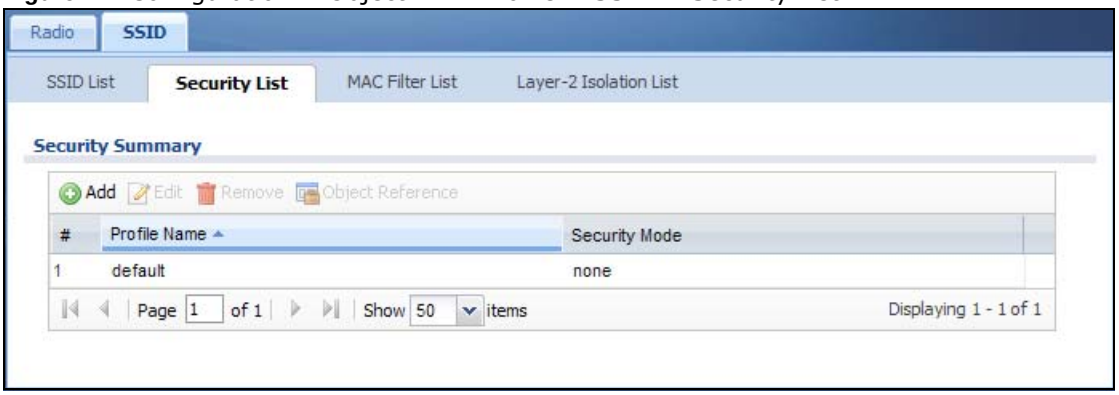
8.3.2 Security List

This screen allows you to manage wireless security configurations that can be used by your SSIDs. Wireless security is implemented strictly between the AP broadcasting the SSID and the stations that are connected to it.

To access this screen click **Configuration > Object > AP Profile > SSID > Security List**.

Note: You can have a maximum of 32 security profiles on the NWA.

Figure 44 Configuration > Object > AP Profile > SSID > Security List



The following table describes the labels in this screen.

Table 38 Configuration > Object > AP Profile > SSID > Security List

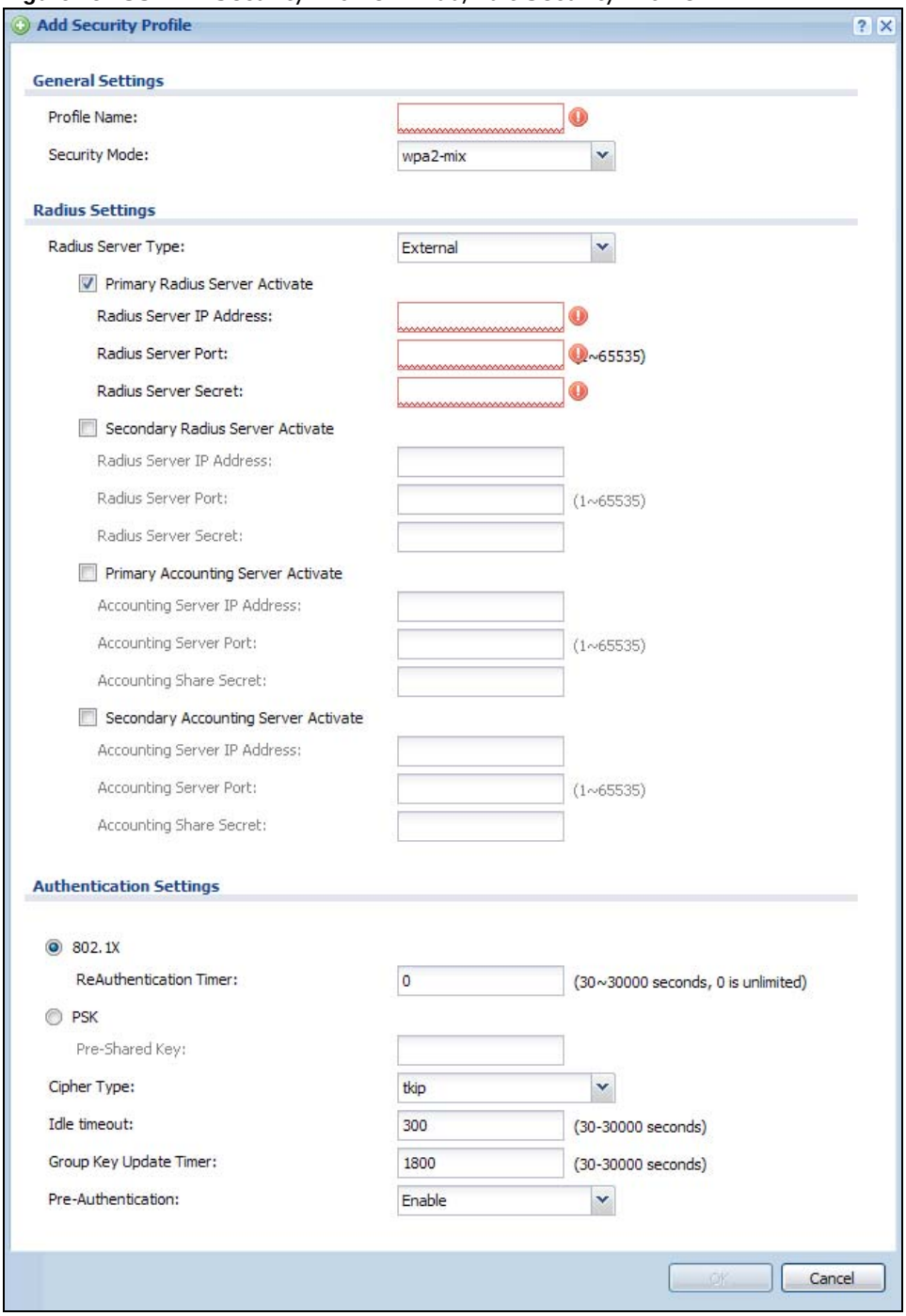
LABEL	DESCRIPTION
Add	Click this to add a new security profile.
Edit	Click this to edit the selected security profile.
Remove	Click this to remove the selected security profile.
Object Reference	Click this to view which other objects are linked to the selected security profile (for example, SSID profile).
#	This field is a sequential value, and it is not associated with a specific user.
Profile Name	This field indicates the name assigned to the security profile.
Security Mode	This field indicates this profile's security mode (if any).

8.3.2.1 Add/Edit Security Profile

This screen allows you to create a new security profile or edit an existing one. To access this screen, click the **Add** button or select a security profile from the list and click the **Edit** button.

Note: This screen's options change based on the Security Mode selected. Only the default screen is displayed here.

Figure 45 SSID > Security Profile > Add/Edit Security Profile



The following table describes the labels in this screen.

Table 39 SSID > Security Profile > Add/Edit Security Profile

LABEL	DESCRIPTION
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Security Mode	Select a security mode from the list: **none**, **wep**, **wpa**, **wpa2**, or **wpa2-mix**.
Radius Server Type	This shows **External** and the NWA uses an external RADIUS server for authentication.
Primary / Secondary Radius Server Activate	Select this to have the NWA use the specified RADIUS server.
Radius Server IP Address	Enter the IP address of the RADIUS server to be used for authentication.
Radius Server Port	Enter the port number of the RADIUS server to be used for authentication.
Radius Server Secret	Enter the shared secret password of the RADIUS server to be used for authentication.
Primary / Secondary Accounting Server Activate	Select the check box to enable user accounting through an external authentication server.
Accounting Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Accounting Server Port	Enter the port number of the external accounting server. The default port number is 1813. You need not change this value unless your network administrator instructs you to do so with additional information.
Accounting Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external accounting server and the NWA. The key must be the same on the external accounting server and your NWA. The key is not sent over the network.
802.1X	Select this to enable 802.1x secure authentication.
ReAuthentication Timer	Enter the interval (in seconds) between authentication requests. Enter a 0 for unlimited requests.
Idle Timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Authentication Type	Select a WEP authentication method. Choices are **Open** or **Share** key. **Share** key is only available if you are not using 802.1x.
Key Length	Select the bit-length of the encryption key to be used in WEP connections. If you select **WEP-64**: • Enter 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x11AA22BB33) for each **Key** used. or • Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for each **Key** used. If you select **WEP-128**: • Enter 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x00112233445566778899AABBCC) for each **Key** used. or • Enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for each **Key** used.

Table 39 SSID > Security Profile > Add/Edit Security Profile (continued)

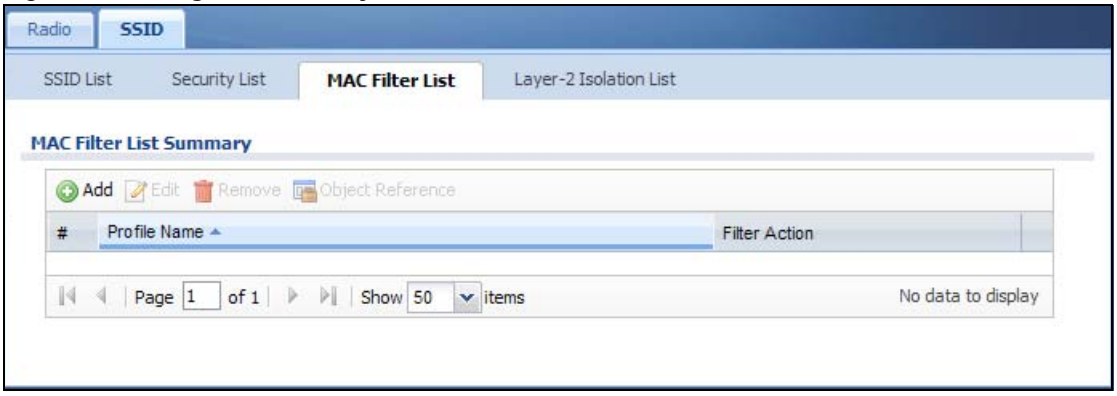
LABEL	DESCRIPTION
Key 1~4	Based on your **Key Length** selection, enter the appropriate length hexadecimal or ASCII key.
PSK	This field is available when you select the **wpa**, **wpa2**, or **wpa2-mix** security mode. Select this option to use a Pre-Shared Key with WPA encryption.
Pre-Shared Key	Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
Cipher Type	Select an encryption cipher type from the list. • **auto** - This automatically chooses the best available cipher based on the cipher in use by the wireless client that is attempting to make a connection. • **tkip** - This is the Temporal Key Integrity Protocol encryption method added later to the WEP encryption protocol to further secure. Not all wireless clients may support this. • **aes** - This is the Advanced Encryption Standard encryption method. It is a more recent development over TKIP and considerably more robust. Not all wireless clients may support this.
Group Key Update Timer	Enter the interval (in seconds) at which the AP updates the group WPA encryption key.
Pre-Authentication	This is available when the profile is set to use **wpa2** or **wpa2-mix** and 802.1x. **Enable** or **Disable** pre-authentication to allow the NWA to send authentication information to other APs on the network, allowing connected wireless clients to switch APs without having to re-authenticate their network connection.
OK	Click **OK** to save your changes back to the NWA.
Cancel	Click **Cancel** to exit this screen without saving your changes.

8.3.3 MAC Filter List

This screen allows you to create and manage security configurations that can be used by your SSIDs. To access this screen click **Configuration > Object > AP Profile > SSID > MAC Filter List**.

Note: You can have a maximum of 32 MAC filtering profiles on the NWA.

Figure 46 Configuration > Object > AP Profile > SSID > MAC Filter List



The following table describes the labels in this screen.

Table 40 Configuration > Object > AP Profile > SSID > MAC Filter List

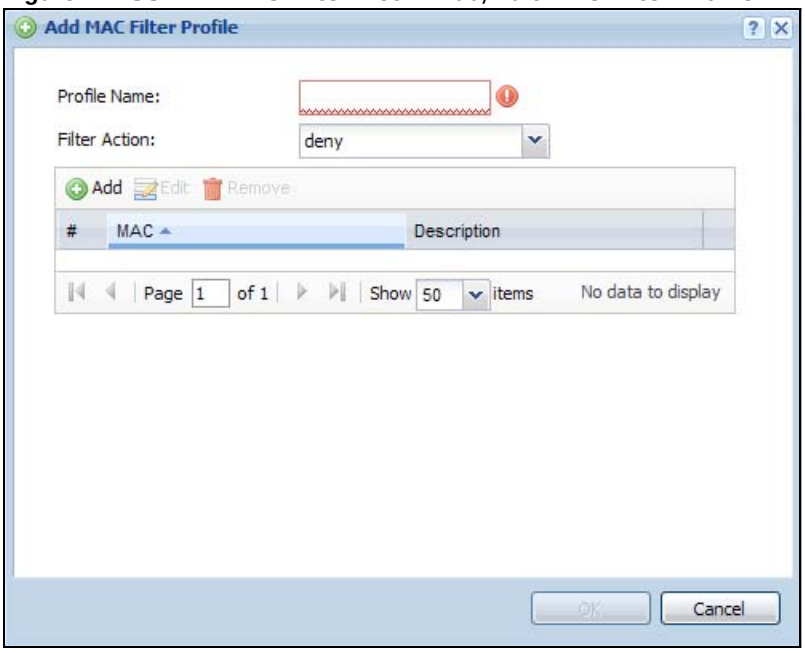
LABEL	DESCRIPTION
Add	Click this to add a new MAC filtering profile.
Edit	Click this to edit the selected MAC filtering profile.
Remove	Click this to remove the selected MAC filtering profile.
Object Reference	Click this to view which other objects are linked to the selected MAC filtering profile (for example, SSID profile).
#	This field is a sequential value, and it is not associated with a specific user.
Profile Name	This field indicates the name assigned to the MAC filtering profile.
Filter Action	This field indicates this profile's filter action (if any).

8.3.3.1 Add/Edit MAC Filter Profile

This screen allows you to create a new MAC filtering profile or edit an existing one. To access this screen, click the **Add** button or select a MAC filter profile from the list and click the **Edit** button.

Note: Each MAC filtering profile can include a maximum of 512 MAC addresses.

Figure 47 SSID > MAC Filter List > Add/Edit MAC Filter Profile



The following table describes the labels in this screen.

Table 41 SSID > MAC Filter List > Add/Edit MAC Filter Profile

LABEL	DESCRIPTION
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Filter Action	Select **allow** to permit the wireless client with the MAC addresses in this profile to connect to the network through the associated SSID; select **deny** to block the wireless clients with the specified MAC addresses.

Table 41 SSID > MAC Filter List > Add/Edit MAC Filter Profile (continued)

LABEL	DESCRIPTION
Add	Click this to add a MAC address to the profile's list.
Edit	Click this to edit the selected MAC address in the profile's list.
Remove	Click this to remove the selected MAC address from the profile's list.
#	This field is a sequential value, and it is not associated with a specific user.
MAC	This field specifies a MAC address associated with this profile.
Description	This field displays a description for the MAC address associated with this profile. You can click the description to make it editable. Enter up to 60 characters, spaces and underscores allowed.
OK	Click **OK** to save your changes back to the NWA.
Cancel	Click **Cancel** to exit this screen without saving your changes.

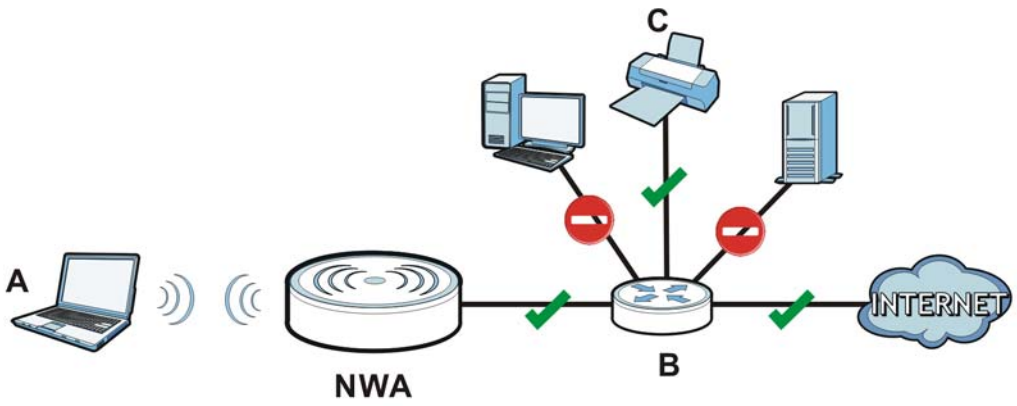
8.3.4 Layer-2 Isolation List

Layer-2 isolation is used to prevent wireless clients associated with your NWA from communicating with other wireless clients, APs, computers or routers in a network.

In the following example, layer-2 isolation is enabled on the NWA to allow a guest wireless client (**A**) to access the main network router (**B**). The router provides access to the Internet and the network printer (**C**) while preventing the client from accessing other computers and servers on the network. The client can communicate with other wireless clients only if Intra-BSS Traffic blocking is disabled.

Note: Intra-BSS Traffic Blocking is activated when you enable layer-2 isolation.

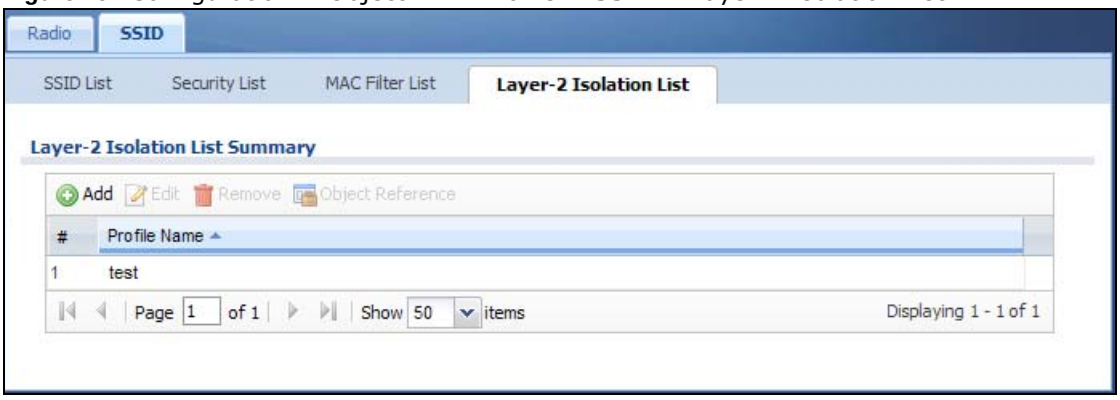
Figure 48 Layer-2 Isolation Application



MAC addresses that are not listed in the layer-2 isolation table are blocked from communicating with the NWA's wireless clients except for broadcast packets. Layer-2 isolation does not check the traffic between wireless clients that are associated with the same AP. Intra-BSS traffic allows wireless clients associated with the same AP to communicate with each other.

This screen allows you to specify devices you want the users on your wireless networks to access. To access this screen click **Configuration > Object > AP Profile > SSID > Layer-2 Isolation List**.

Figure 49 Configuration > Object > AP Profile > SSID > Layer-2 Isolation List



The following table describes the labels in this screen.

Table 42 Configuration > Object > AP Profile > SSID > Layer-2 Isolation List

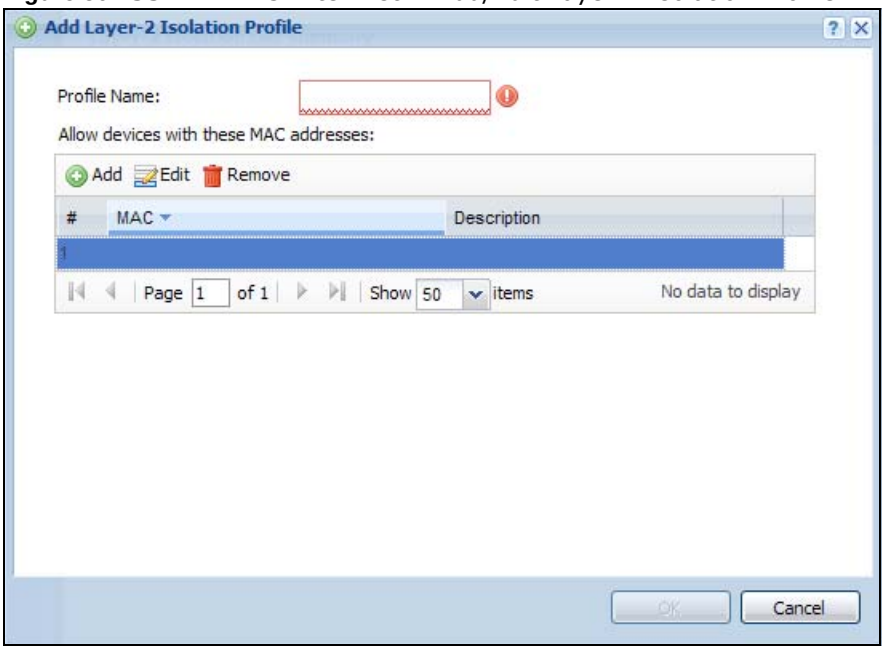
LABEL	DESCRIPTION
Add	Click this to add a new MAC filtering profile.
Edit	Click this to edit the selected MAC filtering profile.
Remove	Click this to remove the selected MAC filtering profile.
Object Reference	Click this to view which other objects are linked to the selected MAC filtering profile (for example, SSID profile).
#	This field is a sequential value, and it is not associated with a specific user.
Profile Name	This field indicates the name assigned to the layer-2 isolation profile.

8.3.4.1 Add/Edit Layer-2 Isolation Profile

This screen allows you to create a new layer-2 isolation profile or edit an existing one. To access this screen, click the **Add** button or select a layer-2 isolation profile from the list and click the **Edit** button.

Note: You need to know the MAC address of each wireless client, AP, computer or router that you want to allow to communicate with the NWA's wireless clients.

Figure 50 SSID > MAC Filter List > Add/Edit Layer-2 Isolation Profile



The following table describes the labels in this screen.

Table 43 SSID > MAC Filter List > Add/Edit Layer-2 Isolation Profile

LABEL	DESCRIPTION
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Add	Click this to add a MAC address to the profile's list.
Edit	Click this to edit the selected MAC address in the profile's list.
Remove	Click this to remove the selected MAC address from the profile's list.
#	This field is a sequential value, and it is not associated with a specific user.
MAC	This field specifies a MAC address associated with this profile.
Description	This field displays a description for the MAC address associated with this profile. You can click the description to make it editable. Enter up to 60 characters, spaces and underscores allowed.
OK	Click **OK** to save your changes back to the NWA.
Cancel	Click **Cancel** to exit this screen without saving your changes.

9

MON Profile

9.1 Overview

This screen allows you to set up monitor mode configurations that allow your NWA to scan for other wireless devices in the vicinity. Once detected, you can use the **Wireless > MON Mode** screen (Section 6.3 on page 55) to classify them as either rogue or friendly.

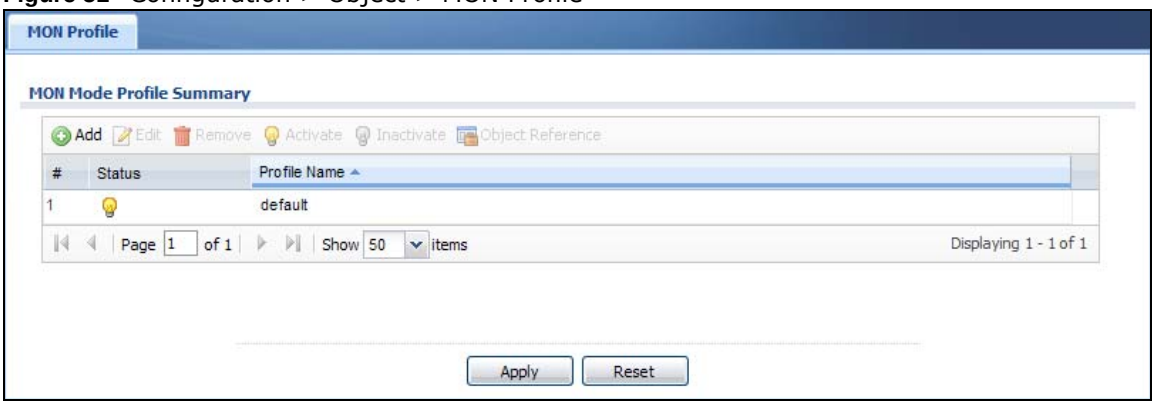
9.1.1 What You Can Do in this Chapter

The **MON Profile** screen (Section 9.2 on page 91) creates preset monitor mode configurations that can be used by the NWA.

9.2 MON Profile

This screen allows you to create monitor mode configurations that can be used by the APs. To access this screen, login to the Web Configurator, and click **Configuration > Object > MON Profile**.

Figure 51 Configuration > Object > MON Profile



The following table describes the labels in this screen.

Table 44 Configuration > Object > MON Profile

LABEL	DESCRIPTION
Add	Click this to add a new monitor mode profile.
Edit	Click this to edit the selected monitor mode profile.
Remove	Click this to remove the selected monitor mode profile.
Activate	To turn on an entry, select it and click **Activate**.

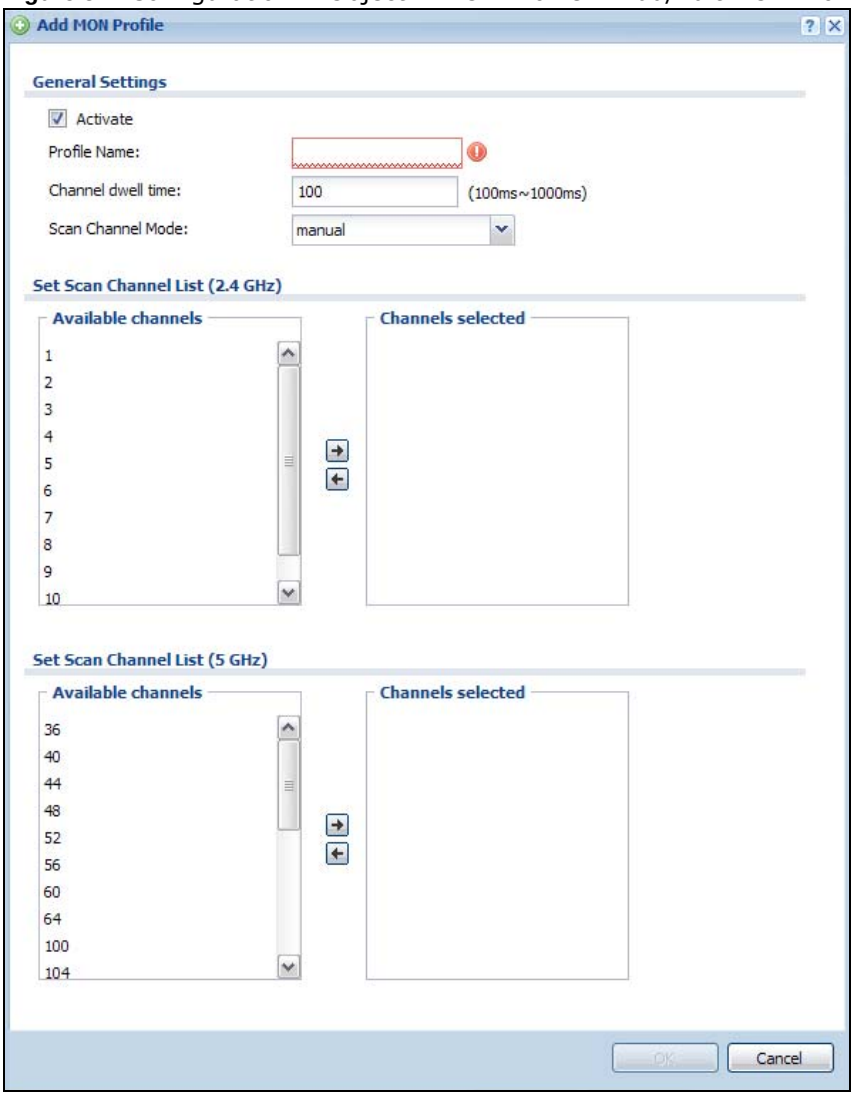
Table 44 Configuration > Object > MON Profile (continued)

LABEL	DESCRIPTION
Inactivate	To turn off an entry, select it and click **Inactivate**.
Object Reference	Click this to view which other objects are linked to the selected monitor mode profile (for example, an AP management profile).
#	This field is a sequential value, and it is not associated with a specific profile.
Status	This field shows whether or not the entry is activated.
Profile Name	This field indicates the name assigned to the monitor profile.

9.2.1 Add/Edit MON Profile

This screen allows you to create a new monitor mode profile or edit an existing one. To access this screen, click the **Add** button or select and existing monitor mode profile and click the **Edit** button.

Figure 52 Configuration > Object > MON Profile > Add/Edit MON Profile



The following table describes the labels in this screen.

Table 45 Configuration > Object > MON Profile > Add/Edit MON Profile

LABEL	DESCRIPTION
Activate	Select this to activate this monitor mode profile.
Profile Name	This field indicates the name assigned to the monitor mode profile.
Channel dwell time	Enter the interval (in milliseconds) before the NWA switches to another channel for monitoring.
Scan Channel Mode	Select **auto** to have the NWA switch to the next sequential channel once the **Channel dwell time** expires. Select **manual** to set specific channels through which to cycle sequentially when the **Channel dwell time** expires. Selecting this options makes the **Scan Channel List** options available.
Set Scan Channel List (2.4 GHz)	Move a channel from the **Available channels** column to the **Channels selected** column to have the NWA using this profile scan that channel when **Scan Channel Mode** is set to **manual**. These channels are limited to the 2.4 GHz range (802.11 b/g/n).
Set Scan Channel List (5 GHz)	Move a channel from the **Available channels** column to the **Channels selected** column to have the NWA using this profile scan that channel when **Scan Channel Mode** is set to **manual**. These channels are limited to the 5 GHz range (802.11 a/n).
OK	Click **OK** to save your changes back to the NWA.
Cancel	Click **Cancel** to exit this screen without saving your changes.

9.3 Technical Reference

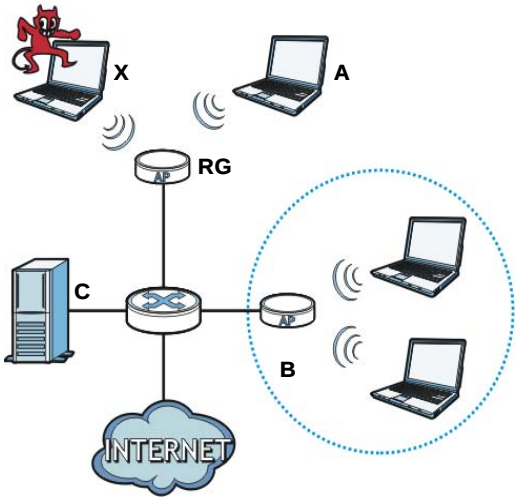
The following section contains additional technical information about the features described in this chapter.

Rogue APs

Rogue APs are wireless access points operating in a network's coverage area that are not under the control of the network's administrators, and can open up holes in a network's security. Attackers can take advantage of a rogue AP's weaker (or non-existent) security to gain access to the network,

or set up their own rogue APs in order to capture information from wireless clients. If a scan reveals a rogue AP, you can use commercially-available software to physically locate it.

Figure 53 Rogue AP Example



In the example above, a corporate network's security is compromised by a rogue AP (**RG**) set up by an employee at his workstation in order to allow him to connect his notebook computer wirelessly (**A**). The company's legitimate wireless network (the dashed ellipse **B**) is well-secured, but the rogue AP uses inferior security that is easily broken by an attacker (**X**) running readily available encryption-cracking software. In this example, the attacker now has access to the company network, including sensitive data stored on the file server (**C**).

Friendly APs

If you have more than one AP in your wireless network, you should also configure a list of "friendly" APs. Friendly APs are other wireless access points that are detected in your network, as well as any others that you know are not a threat (those from recognized networks, for example). It is recommended that you export (save) your list of friendly APs often, especially if you have a network with a large number of access points.

10

Certificates

10.1 Overview

The NWA can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

10.1.1 What You Can Do in this Chapter

- The **My Certificate** screens (Section 10.2 on page 98) generate and export self-signed certificates or certification requests and import the NWA's CA-signed certificates.
- The **Trusted Certificates** screens (Section 10.3 on page 106) save CA certificates and trusted remote host certificates to the NWA. The NWA trusts any valid certificate that you have imported as a trusted certificate. It also trusts any valid certificate signed by any of the certificates that you have imported as a trusted certificate.

10.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as "digital signatures"). Only you can write your signature exactly as it should look. When people know what your signature looks like, they can verify whether something was signed by you, or by someone else. In the same way, your private key "writes" your digital signature and your public key allows people to verify whether data was signed by you, or by someone else.

This process works as follows:

1. Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).
2. Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.
3. Tim uses his private key to sign the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim's private key).

5 Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny's public key to verify the message.

The NWA uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The NWA does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The NWA can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

Advantages of Certificates

Certificates offer the following benefits.

- The NWA only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Self-signed Certificates

You can have the NWA act as a certification authority and sign its own certificates.

Factory Default Certificate

The NWA generates its own unique self-signed certificate when you first turn it on. This certificate is referred to in the GUI as the factory default certificate.

Certificate File Formats

Any certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The NWA currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.

- Binary PKCS#12: This is a format for transferring public key and private key certificates.The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the NWA.

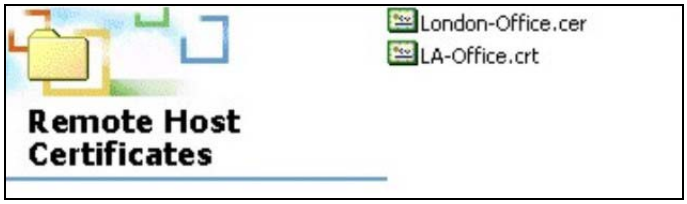
Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

10.1.3 Verifying a Certificate

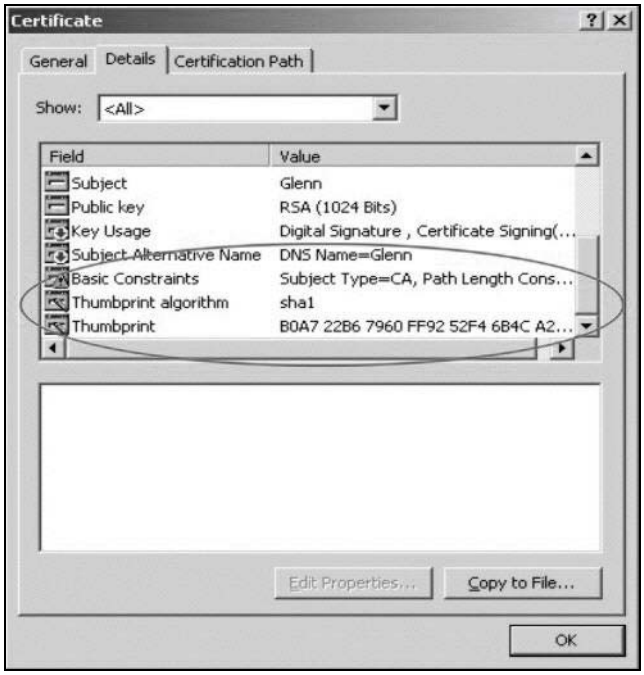
Before you import a trusted certificate into the NWA, you should verify that you have the correct certificate. You can do this using the certificate's fingerprint. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithm. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1 Browse to where you have the certificate saved on your computer.

2 Make sure that the certificate has a ".cer" or ".crt" file name extension.



3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

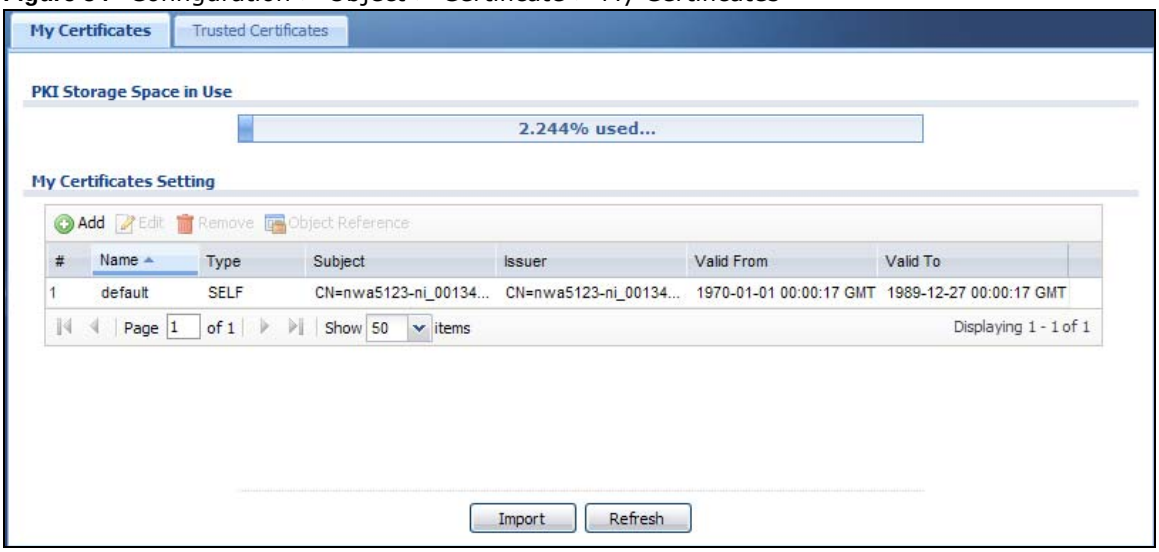


4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

10.2 My Certificates

Click **Configuration > Object > Certificate > My Certificates** to open this screen. This is the NWA's summary list of certificates and certification requests.

Figure 54 Configuration > Object > Certificate > My Certificates



The following table describes the labels in this screen.

Table 46 Configuration > Object > Certificate > My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the NWA's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Add	Click this to go to the screen where you can have the NWA generate a certificate or a certification request.
Edit	Double-click an entry or select it and click **Edit** to open a screen with an in-depth list of information about the certificate.
Remove	The NWA keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click **Remove**. The NWA confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
Object Reference	You cannot delete certificates that any of the NWA's features are configured to use. Select an entry and click **Object Reference** to open a screen that shows which settings use the entry.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. **CERT** represents a certificate issued by a certification authority.

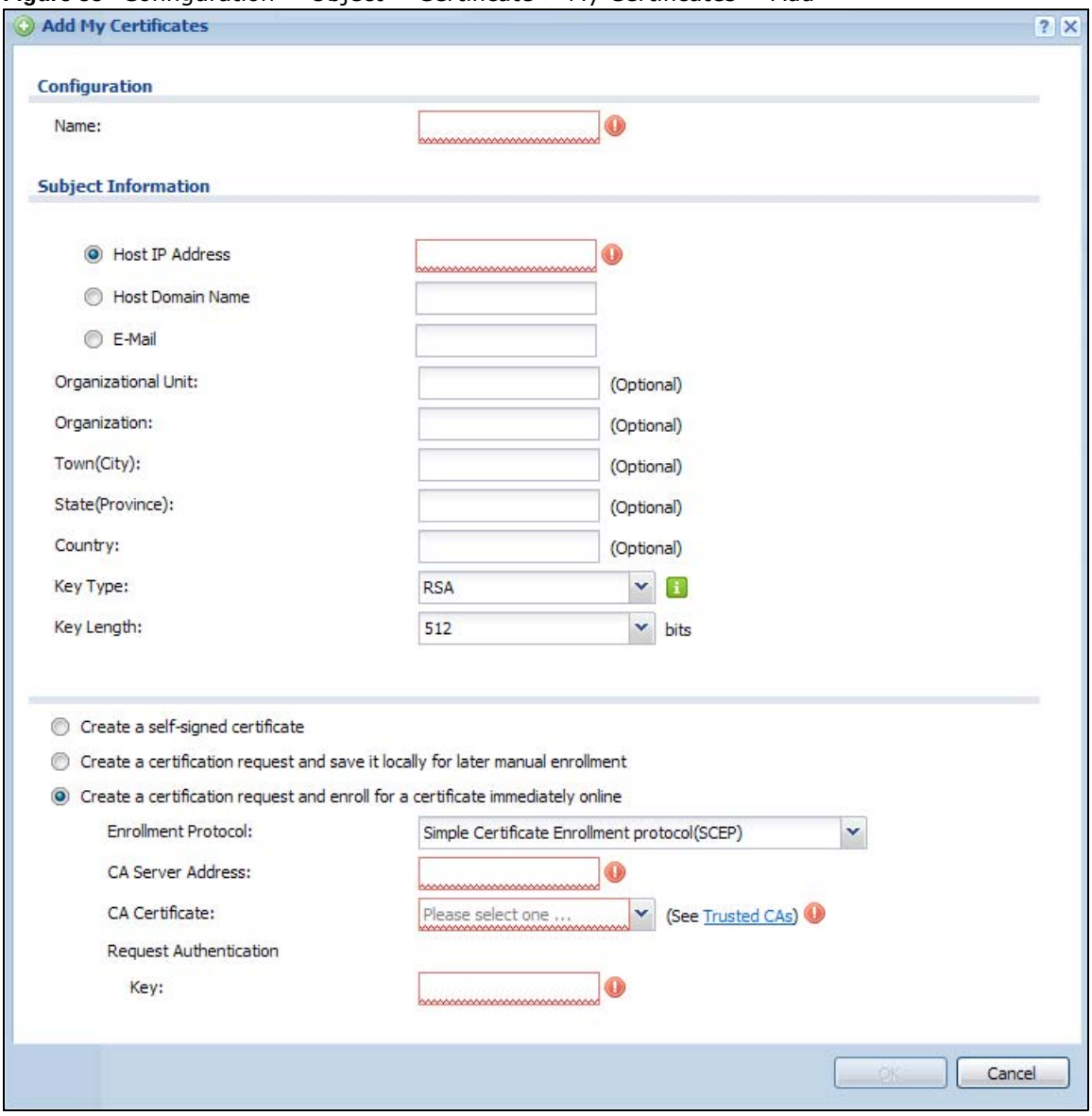
Table 46 Configuration > Object > Certificate > My Certificates (continued)

LABEL	DESCRIPTION
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click **Import** to open a screen where you can save a certificate to the NWA.
Refresh	Click **Refresh** to display the current validity status of the certificates.

10.2.1 Add My Certificates

Click **Configuration > Object > Certificate > My Certificates** and then the **Add** icon to open the **Add My Certificates** screen. Use this screen to have the NWA create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Figure 55 Configuration > Object > Certificate > My Certificates > Add



The following table describes the labels in this screen.

Table 47 Configuration > Object > Certificate > My Certificates > Add

LABEL	DESCRIPTION
Name	Type a name to identify this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although you must specify a **Host IP Address**, **Host Domain Name**, or **E-Mail**. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information. Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address is for identification purposes only and can be any string. A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods. An e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.
Organizational Unit	Identify the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Organization	Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Town (City)	Identify the town or city where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
State (Province)	Identify the state or province where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Country	Identify the nation where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Key Type	Select **RSA** to use the Rivest, Shamir and Adleman public-key algorithm. Select **DSA** to use the Digital Signature Algorithm public-key algorithm.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select this to have the NWA generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select this to have the NWA generate and store a request for a certificate. Use the **My Certificate Edit** screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the **My Certificate Edit** screen and then send it to the certification authority.

Table 47 Configuration > Object > Certificate > My Certificates > Add (continued)

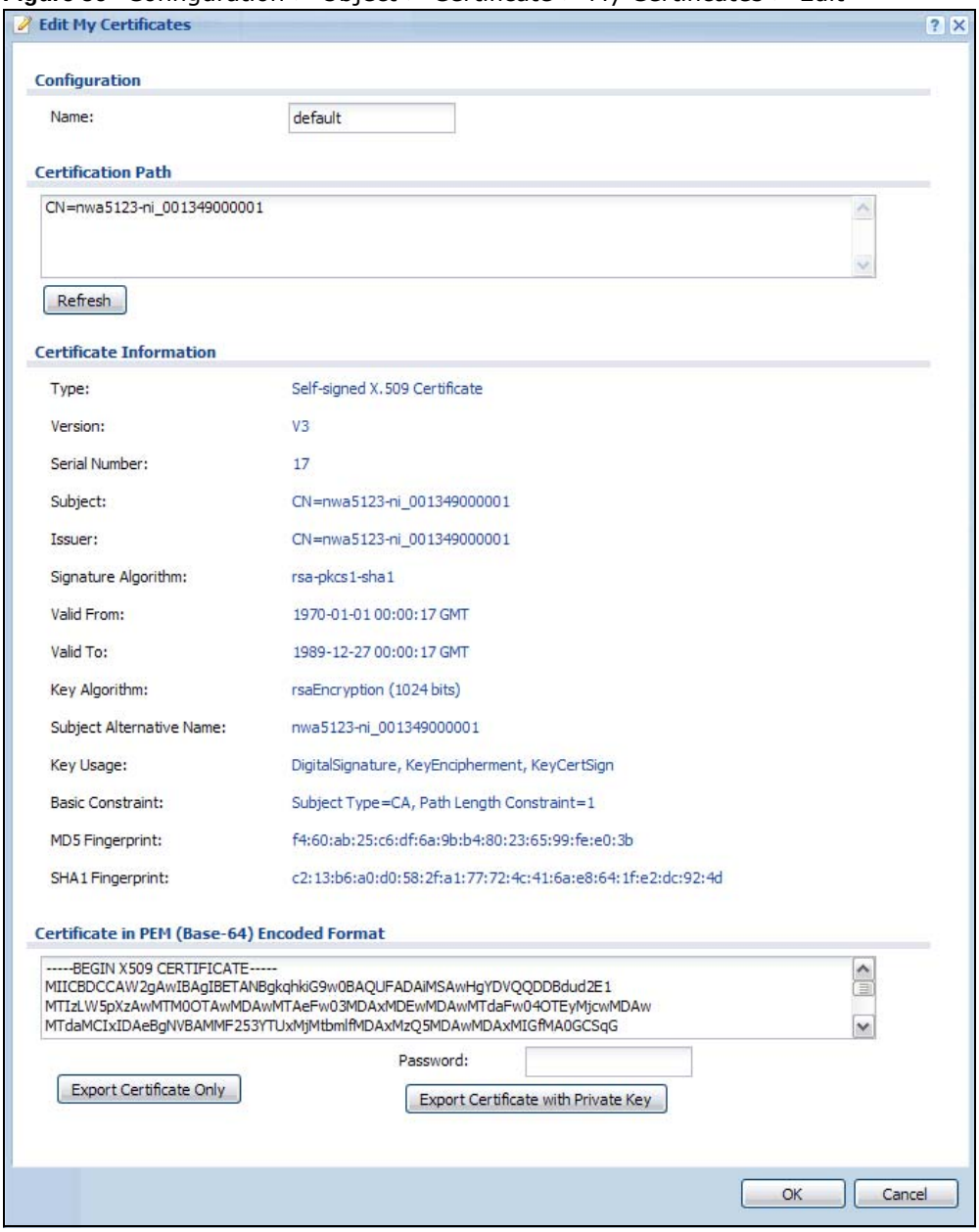
LABEL	DESCRIPTION
Create a certification request and enroll for a certificate immediately online	Select this to have the NWA generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the **Trusted Certificates** screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the **Reference Number** and **Key** if the certification authority requires them.
Enrollment Protocol	This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Select the certification authority's enrollment protocol from the drop-down list box. **Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. **Certificate Management Protocol (CMP)** is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Enter the IP address (or URL) of the certification authority server. For a URL, you can use up to 511 of the following characters. a-zA-Z0-9'()+,/ :.=?;!*#@$_%-
CA Certificate	This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Select the certification authority's certificate from the **CA Certificate** drop-down list box. You must have the certification authority's certificate already imported in the **Trusted Certificates** screen. Click **Trusted CAs** to go to the **Trusted Certificates** screen where you can view (and manage) the NWA's list of certificates of trusted certification authorities.
Request Authentication	When you select **Create a certification request and enroll for a certificate immediately online**, the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the **Reference Number** and the **Key** fields if your certification authority uses the CMP enrollment protocol. Just the **Key** field displays if your certification authority uses the SCEP enrollment protocol. For the reference number, use 0 to 99999999. For the key, use up to 31 of the following characters. a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-
OK	Click **OK** to begin certificate or certification request generation.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

If you configured the **Add My Certificates** screen to have the NWA enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **Add My Certificates** screen. Click **Return** and check your information in the **Add My Certificates** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the NWA to enroll a certificate online.

10.2.2 Edit My Certificates

Click **Configuration > Object > Certificate > My Certificates** and then the **Edit** icon to open the **My Certificate Edit** screen. You can use this screen to view in-depth certificate information and change the certificate's name.

Figure 56 Configuration > Object > Certificate > My Certificates > Edit



The following table describes the labels in this screen.

Table 48 Configuration > Object > Certificate > My Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Certification Path	This field displays for a certificate, not a certification request. Click the **Refresh** button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The NWA does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number. "
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the NWA.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O), State (ST), and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the **Subject Name** field. "none" displays for a certification request.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The NWA uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. "none" displays for a certification request.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. "none" displays for a certification request.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the NWA uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. This field does not display for a certification request.

Table 48 Configuration > Object > Certificate > My Certificates > Edit

LABEL	DESCRIPTION
MD5 Fingerprint	This is the certificate's message digest that the NWA calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the NWA calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export Certificate Only	Use this button to save a copy of the certificate without its private key. Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Password	If you want to export the certificate with its private key, create a password and type it here. Make sure you keep this password in a safe place. You will need to use it if you import the certificate to another device.
Export Certificate with Private Key	Use this button to save a copy of the certificate with its private key. Type the certificate's password and click this button. Click **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
OK	Click **OK** to save your changes back to the NWA. You can only change the name.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

10.2.3 Import Certificates

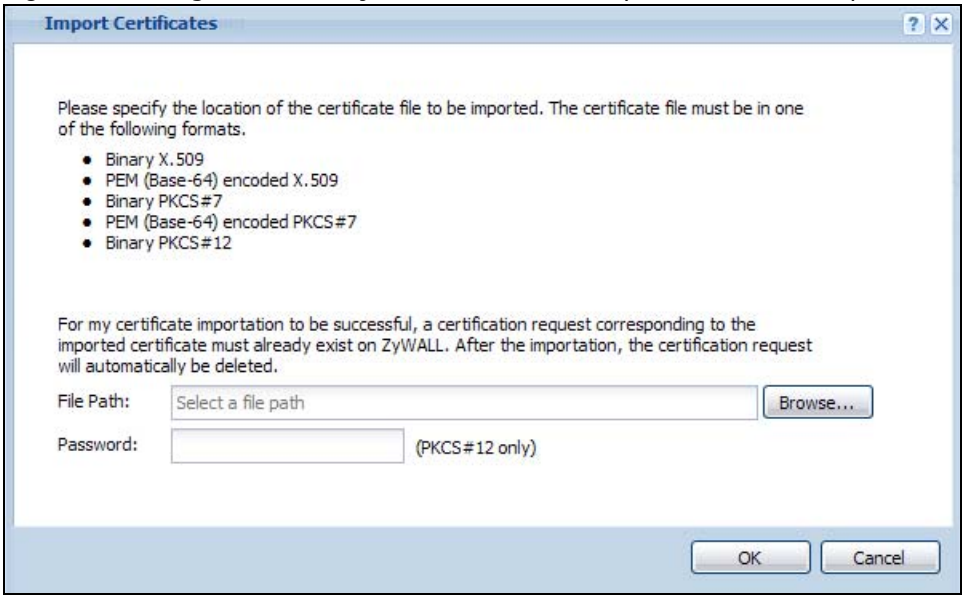
Click **Configuration > Object > Certificate > My Certificates > Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the NWA.

Note: You can import a certificate that matches a corresponding certification request that was generated by the NWA. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.

The certificate you import replaces the corresponding request in the **My Certificates** screen.

You must remove any spaces in the certificate's filename before you can import it.

Figure 57 Configuration > Object > Certificate > My Certificates > Import


Import Certificates
Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.
Binary X.509
PEM (Base-64) encoded X.509
Binary PKCS#7
PEM (Base-64) encoded PKCS#7
Binary PKCS#12
For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyWALL. After the importation, the certification request will automatically be deleted.
File Path:
Select a file path
Browse...
Password:
(PKCS#12 only)
OK
Cancel

The following table describes the labels in this screen.

Table 49 Configuration > Object > Certificate > My Certificates > Import

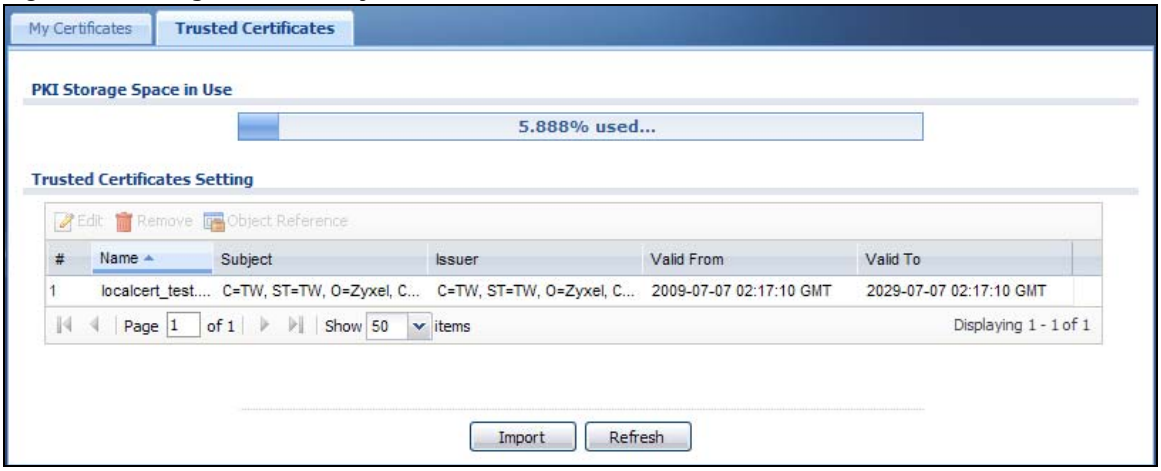
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it. You cannot import a certificate with the same name as a certificate that is already in the NWA.
Browse	Click **Browse** to find the certificate file you want to upload.
Password	This field only applies when you import a binary PKCS#12 format file. Type the file's password that was created when the PKCS #12 file was exported.
OK	Click **OK** to save the certificate on the NWA.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

10.3 Trusted Certificates

Click **Configuration > Object > Certificate > Trusted Certificates** to open the **Trusted Certificates** screen. This screen displays a summary list of certificates that you have set the NWA to accept as trusted. The NWA also accepts any valid certificate signed by a certificate on this list as

being trustworthy; thus you do not need to import any certificate that is signed by one of these certificates.

Figure 58 Configuration > Object > Certificate > Trusted Certificates



The following table describes the labels in this screen.

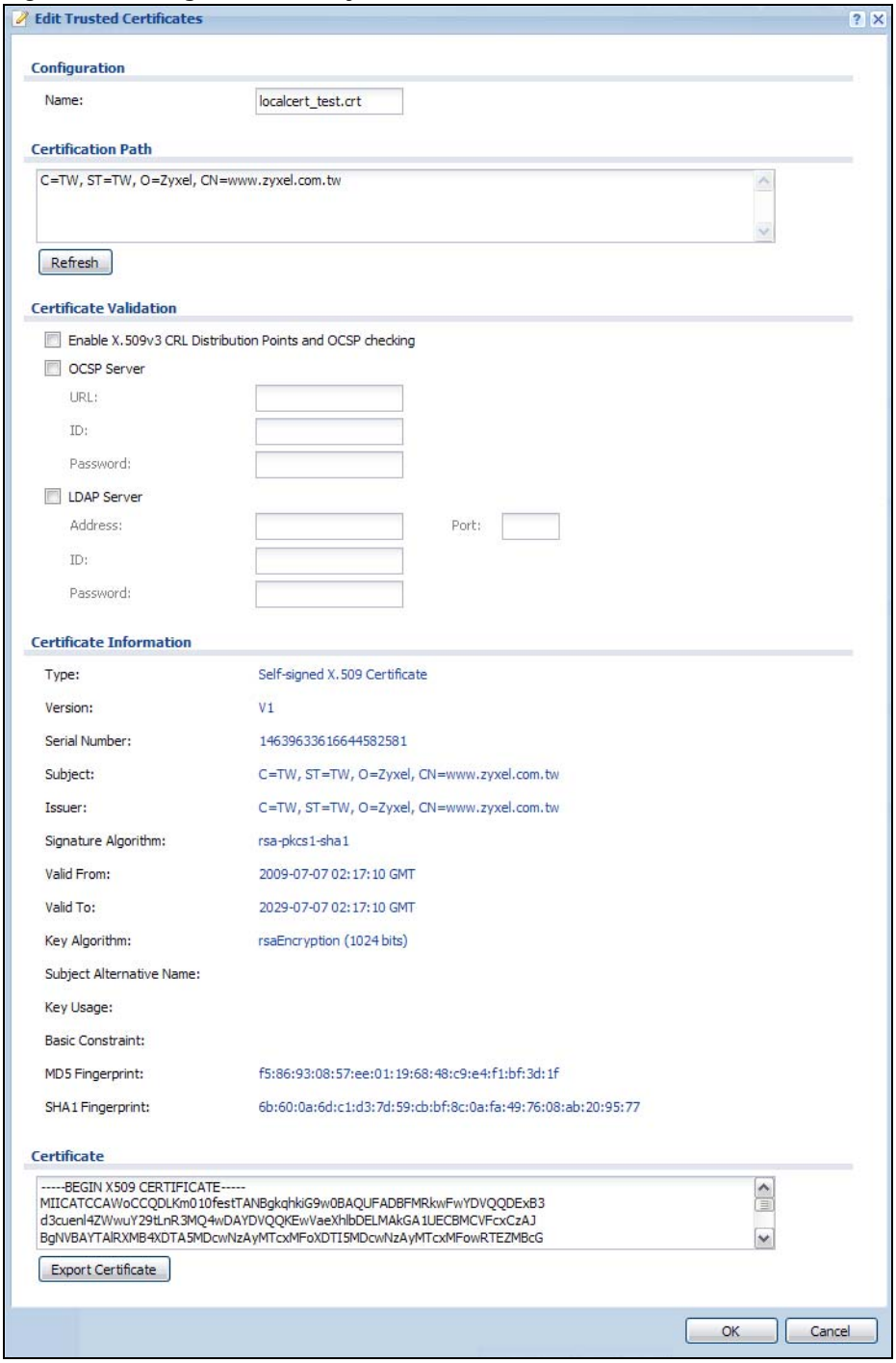
Table 50 Configuration > Object > Certificate > Trusted Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the NWA's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Edit	Double-click an entry or select it and click **Edit** to open a screen with an in-depth list of information about the certificate.
Remove	The NWA keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click **Remove**. The NWA confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
Object Reference	You cannot delete certificates that any of the NWA's features are configured to use. Select an entry and click **Object Reference** to open a screen that shows which settings use the entry.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the NWA.
Refresh	Click this button to display the current validity status of the certificates.

10.3.1 Edit Trusted Certificates

Click **Configuration > Object > Certificate > Trusted Certificates** and then a certificate's **Edit** icon to open the **Trusted Certificates Edit** screen. Use this screen to view in-depth information about the certificate, change the certificate's name and set whether or not you want the NWA to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 59 Configuration > Object > Certificate > Trusted Certificates > Edit



The following table describes the labels in this screen.

Table 51 Configuration > Object > Certificate > Trusted Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can change the name. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Certification Path	Click the **Refresh** button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certificate, it may be the only certification authority in the list (along with the end entity's own certificate). The NWA does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Enable X.509v3 CRL Distribution Points and OCSP checking	Select this check box to have the NWA check incoming certificates that are signed by this certificate against a Certificate Revocation List (CRL) or an OCSP server. You also need to configure the OSCP or LDAP server details.
OCSP Server	Select this check box if the directory server uses OCSP (Online Certificate Status Protocol).
URL	Type the protocol, IP address and pathname of the OCSP server.
ID	The NWA may need to authenticate itself in order to assess the OCSP server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the OCSP server (usually a certification authority).
LDAP Server	Select this check box if the directory server uses LDAP (Lightweight Directory Access Protocol). LDAP is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.
Address	Type the IP address (in dotted decimal notation) of the directory server.
Port	Use this field to specify the LDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
ID	The NWA may need to authenticate itself in order to assess the CRL directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the CRL directory server (usually a certification authority).
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the **Subject Name** field.

Table 51 Configuration > Object > Certificate > Trusted Certificates > Edit (continued)

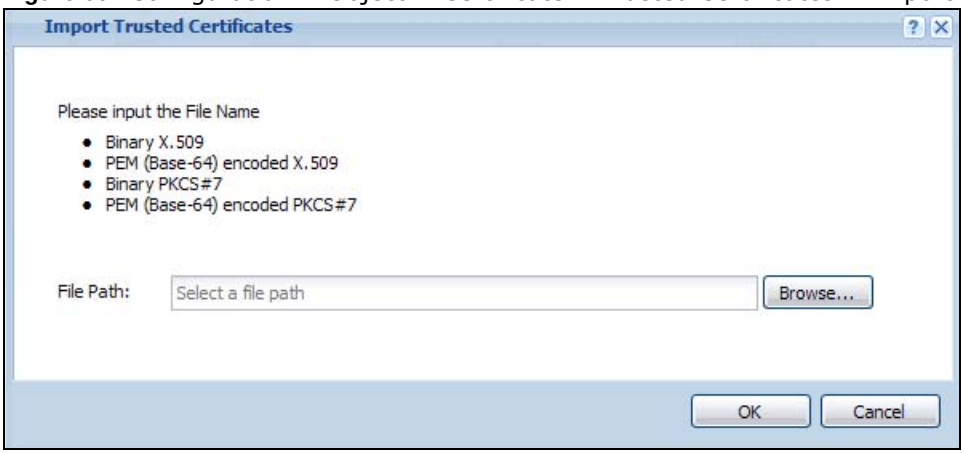
LABEL	DESCRIPTION
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the NWA uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the NWA calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the NWA calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export Certificate	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
OK	Click **OK** to save your changes back to the NWA. You can only change the name.
Cancel	Click **Cancel** to quit and return to the **Trusted Certificates** screen.

10.3.2 Import Trusted Certificates

Click **Configuration > Object > Certificate > Trusted Certificates > Import** to open the **Import Trusted Certificates** screen. Follow the instructions in this screen to save a trusted certificate to the NWA.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 60 Configuration > Object > Certificate > Trusted Certificates > Import



The following table describes the labels in this screen.

Table 52 Configuration > Object > Certificate > Trusted Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it. You cannot import a certificate with the same name as a certificate that is already in the NWA.
Browse	Click **Browse** to find the certificate file you want to upload.
OK	Click **OK** to save the certificate on the NWA.
Cancel	Click **Cancel** to quit and return to the previous screen.

10.4 Technical Reference

The following section contains additional technical information about the features described in this chapter.

OCSP

OCSP (Online Certificate Status Protocol) allows an application or device to check whether a certificate is valid. With OCSP the NWA checks the status of individual certificates instead of downloading a Certificate Revocation List (CRL). OCSP has two main advantages over a CRL. The first is real-time status information. The second is a reduction in network traffic since the NWA only gets information on the certificates that it needs to verify, not a huge list. When the NWA requests certificate status information, the OCSP server returns a "expired", "current" or "unknown" response.

11

System

11.1 Overview

Use the system screens to configure general NWA settings.

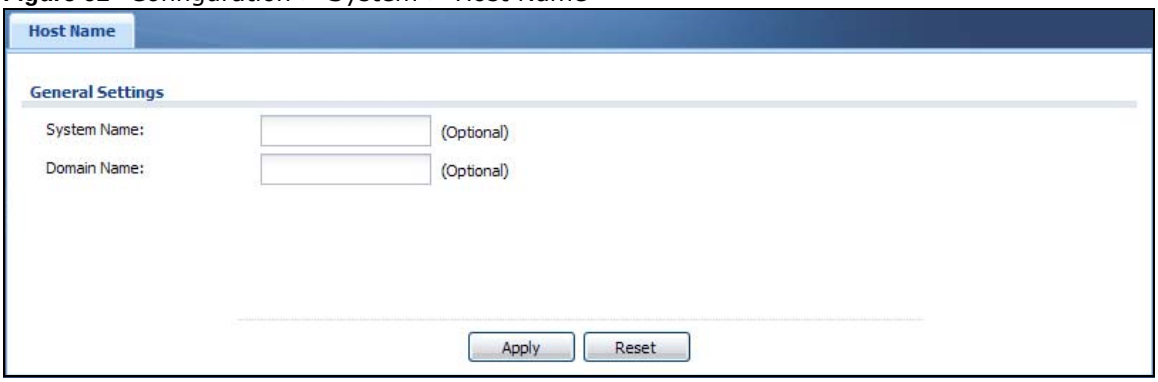
11.1.1 What You Can Do in this Chapter

- The **Host Name** screen (Section 11.2 on page 113) configures a unique name for the NWA in your network.
- The **Date/Time** screen (Section 11.3 on page 114) configures the date and time for the NWA.
- The **WWW** screens (Section 11.4 on page 118) configure settings for HTTP or HTTPS access to the NWA.
- The **SSH** screen (Section 11.5 on page 128) configures SSH (Secure SHell) for securely accessing the NWA's command line interface.
- The **Telnet** screen (Section 11.6 on page 132) configures Telnet for accessing the NWA's command line interface.
- The **FTP** screen (Section 11.7 on page 133) specifies FTP server settings. You can upload and download the NWA's firmware and configuration files using FTP. Please also see Chapter 13 on page 151 for more information about firmware and configuration files.
- The **SNMP** screens (Section 11.8 on page 133) configure the device's SNMP settings, including profiles that define allowed SNMPv3 access.

11.2 Host Name

A host name is the unique name by which a device is known on a network. Click **Configuration > System > Host Name** to open this screen.

Figure 61 Configuration > System > Host Name



The following table describes the labels in this screen.

Table 53 Configuration > System > Host Name

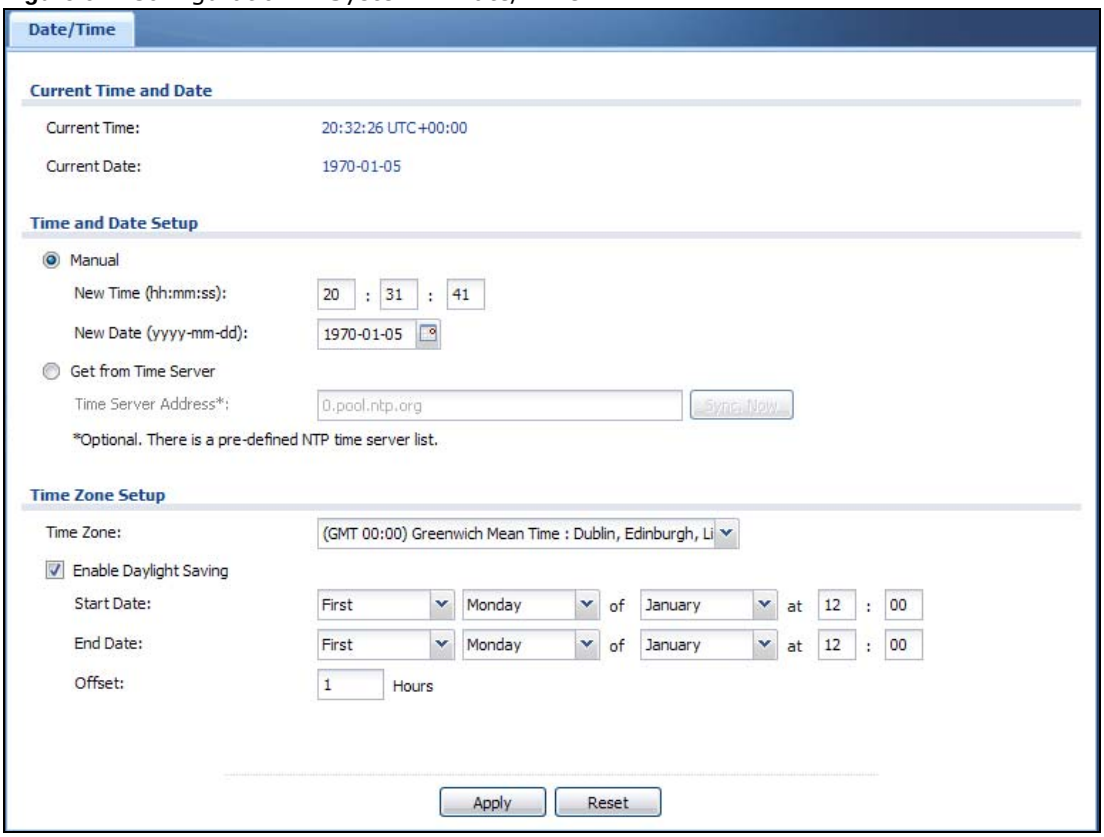
LABEL	DESCRIPTION
System Name	Choose a descriptive name to identify your NWA device. This name can be up to 64 alphanumeric characters long. Spaces are not allowed, but dashes (-) underscores (_) and periods (.) are accepted.
Domain Name	Enter the domain name (if you know it) here. This name is propagated to DHCP clients connected to interfaces with the DHCP server enabled. This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" are accepted.
Apply	Click **Apply** to save your changes back to the NWA.
Reset	Click **Reset** to return the screen to its last-saved settings.

11.3 Date and Time

For effective scheduling and logging, the NWA system time must be accurate. The NWA has a software mechanism to set the time manually or get the current time and date from an external server.

To change your NWA's time based on your local time zone and date, click **Configuration > System > Date/Time**. The screen displays as shown. You can manually set the NWA's time and date or have the NWA get the date and time from a time server.

Figure 62 Configuration > System > Date/Time



The following table describes the labels in this screen.

Table 54 Configuration > System > Date/Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the present time of your NWA.
Current Date	This field displays the present date of your NWA.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, time zone and daylight saving at the same time, the time zone and daylight saving will affect the new time and date you entered. When you enter the time settings manually, the NWA uses the new setting once you click **Apply**.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the NWA get the time and date from the time server you specify below. The NWA requests time and date settings from the time server under the following circumstances. • When the NWA starts up. • When you click **Apply** or **Sync. Now** in this screen. • 24-hour intervals after starting up.
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Sync. Now	Click this button to have the NWA get the time and date from a time server (see the **Time Server Address** field). This also saves your changes (except the daylight saving settings).
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Saving	Daylight saving is a period from late spring to fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **at** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **at** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 54 Configuration > System > Date/Time (continued)

LABEL	DESCRIPTION
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **at** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **at** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Offset	Specify how much the clock changes when daylight saving begins and ends. Enter a number from 1 to 5.5 (by 0.5 increments). For example, if you set this field to 3.5, a log occurred at 6 P.M. in local official time will appear as if it had occurred at 10:30 P.M.
Apply	Click **Apply** to save your changes back to the NWA.
Reset	Click **Reset** to return the screen to its last-saved settings.

11.3.1 Pre-defined NTP Time Servers List

When you turn on the NWA for the first time, the date and time start at 2003-01-01 00:00:00. The NWA then attempts to synchronize with one of the following pre-defined list of Network Time Protocol (NTP) time servers.

The NWA continues to use the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

Table 55 Default Time Servers

0.pool.ntp.org
1.pool.ntp.org
2.pool.ntp.org

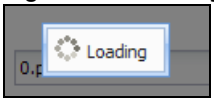
When the NWA uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the NWA goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

11.3.2 Time Server Synchronization

Click the **Sync. Now** button to get the time and date from the time server you specified in the **Time Server Address** field.

When the **Loading** message appears, you may have to wait up to one minute.

Figure 63 Loading



The **Current Time** and **Current Date** fields will display the appropriate settings if the synchronization is successful.

If the synchronization was not successful, a log displays in the **View Log** screen. Try re-configuring the **Date/Time** screen.

To manually set the NWA date and time:

1 Click **System > Date/Time**.

2 Select **Manual** under **Time and Date Setup**.

3 Enter the NWA's time in the **New Time** field.

4 Enter the NWA's date in the **New Date** field.

5 Under **Time Zone Setup**, select your **Time Zone** from the list.

6 As an option you can select the **Enable Daylight Saving** check box to adjust the NWA clock for daylight savings.

7 Click **Apply**.

To get the NWA date and time from a time server:

1 Click **System > Date/Time**.

2 Select **Get from Time Server** under **Time and Date Setup**.

3 Under **Time Zone Setup**, select your **Time Zone** from the list.

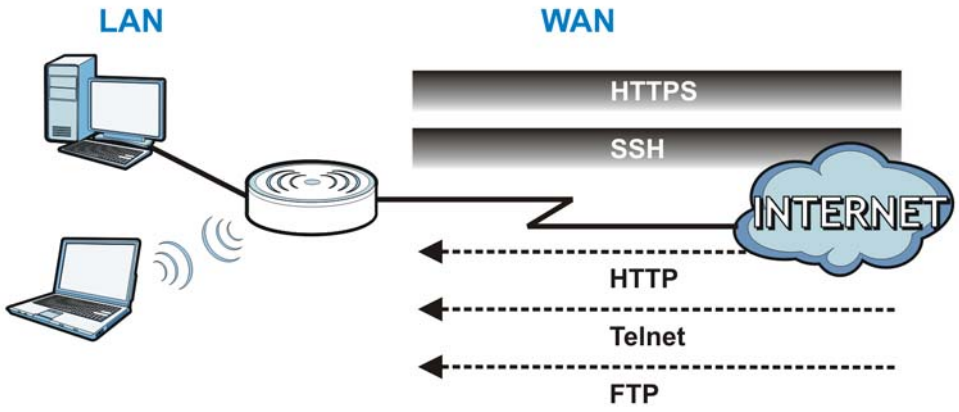
4 Under **Time and Date Setup**, enter a **Time Server Address**.

5 Click **Apply**.

11.4 WWW Overview

The following figure shows secure and insecure management of the NWA coming in from the WAN. HTTPS and SSH access are secure. HTTP, Telnet, and FTP management access are not secure.

Figure 64 Secure and Insecure Service Access From the WAN



11.4.1 Service Access Limitations

A service cannot be used to access the NWA when you have disabled that service in the corresponding screen.

11.4.2 System Timeout

There is a lease timeout for administrators. The NWA automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the NWA for authentication again when the reauthentication time expires.

You can change the timeout settings in the **User** screens.

11.4.3 HTTPS

You can set the NWA to use HTTP or HTTPS (HTTPS adds security) for Web Configurator sessions.

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys (see Chapter 10 on page 95 for more information).

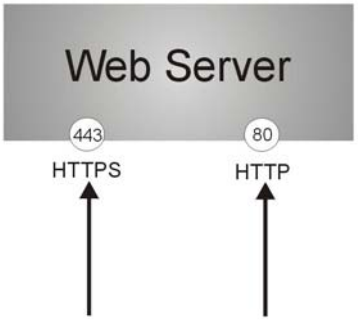
HTTPS on the NWA is used so that you can securely access the NWA using the Web Configurator. The SSL protocol specifies that the HTTPS server (the NWA) must always authenticate itself to the HTTPS client (the computer which requests the HTTPS connection with the NWA), whereas the HTTPS client only should authenticate itself when the HTTPS server requires it to do so (select **Authenticate Client Certificates** in the **WWW** screen). **Authenticate Client Certificates** is optional and if selected means the HTTPS client must send the NWA a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the NWA.

Please refer to the following figure.

1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the NWA's web server.

2 HTTP connection requests from a web browser go to port 80 (by default) on the NWA's web server.

Figure 65 HTTP/HTTPS Implementation

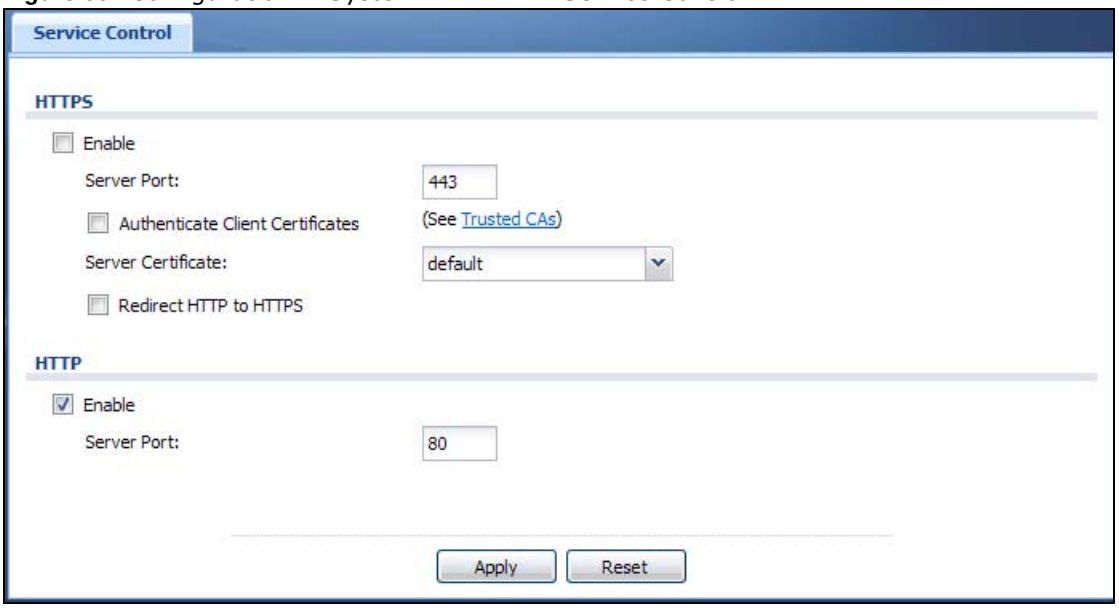


Note: If you disable **HTTP** in the **WWW** screen, then the NWA blocks all HTTP connection attempts.

11.4.4 Configuring WWW Service Control

Click **Configuration > System > WWW** to open the **WWW** screen. Use this screen to specify HTTP or HTTPS settings.

Figure 66 Configuration > System > WWW > Service Control



The following table describes the labels in this screen.

Table 56 Configuration > System > WWW > Service Control

LABEL	DESCRIPTION
HTTPS	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the NWA Web Configurator using secure HTTPs connections.
Server Port	The HTTPS server listens on port 443 by default. If you change the HTTPS server port to a different number on the NWA, for example 8443, then you must notify people who need to access the NWA Web Configurator to use "https://NWA IP Address:**8443**" as the URL.
Authenticate Client Certificates	Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself to the NWA by sending the NWA a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the NWA.
Server Certificate	Select a certificate the HTTPS server (the NWA) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the **My Certificates** screen.
Redirect HTTP to HTTPS	To allow only secure Web Configurator access, select this to redirect all HTTP connection requests to the HTTPS server.
HTTP	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the NWA Web Configurator using HTTP connections.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service to access the NWA.

Table 56 Configuration > System > WWW > Service Control (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the NWA.
Reset	Click **Reset** to return the screen to its last-saved settings.

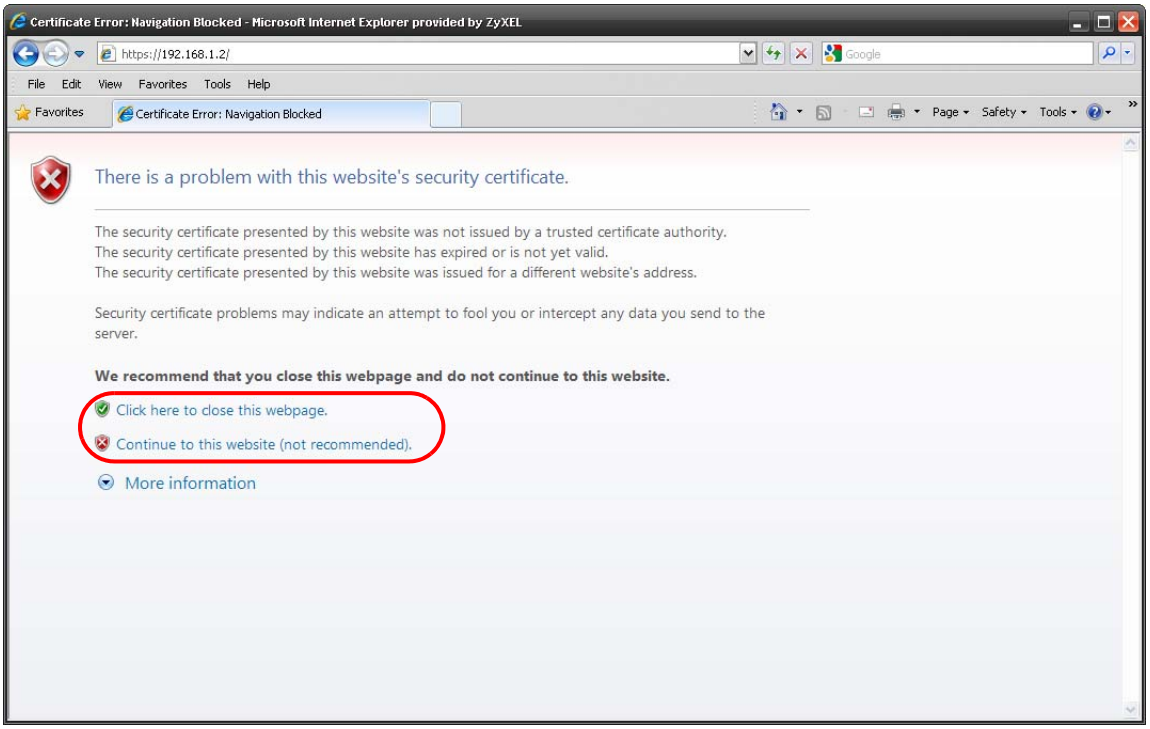
11.4.5 HTTPS Example

If you haven't changed the default HTTPS port on the NWA, then in your browser enter "https://NWA IP Address/" as the web site address where "NWA IP Address" is the IP address or domain name of the NWA you wish to access.

11.4.5.1 Internet Explorer Warning Messages

When you attempt to access the NWA HTTPS server, you will see the error message shown in the following screen.

Figure 67 Security Alert Dialog Box (Internet Explorer)


Certificate Error: Navigation Blocked - Microsoft Internet Explorer provided by ZyXEL
https://192.168.1.2/
File Edit View Favorites Tools Help
Favorites
Certificate Error: Navigation Blocked
Page Safety Tools
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website has expired or is not yet valid.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

Select **Continue to this website.** to proceed to the Web Configurator login screen. Otherwise, select **Click here to close this webpage.** to block the access.

11.4.5.2 Mozilla Firefox Warning Messages

When you attempt to access the NWA HTTPS server, a **The Connection is Untrusted** screen appears as shown in the following screen. Click **Technical Details** if you want to verify more information about the certificate from the NWA.

Select **I Understand the Risks** and then click **Add Exception** to add the NWA to the security exception list. Click **Confirm Security Exception**.

Figure 68 Security Certificate 1 (Firefox)

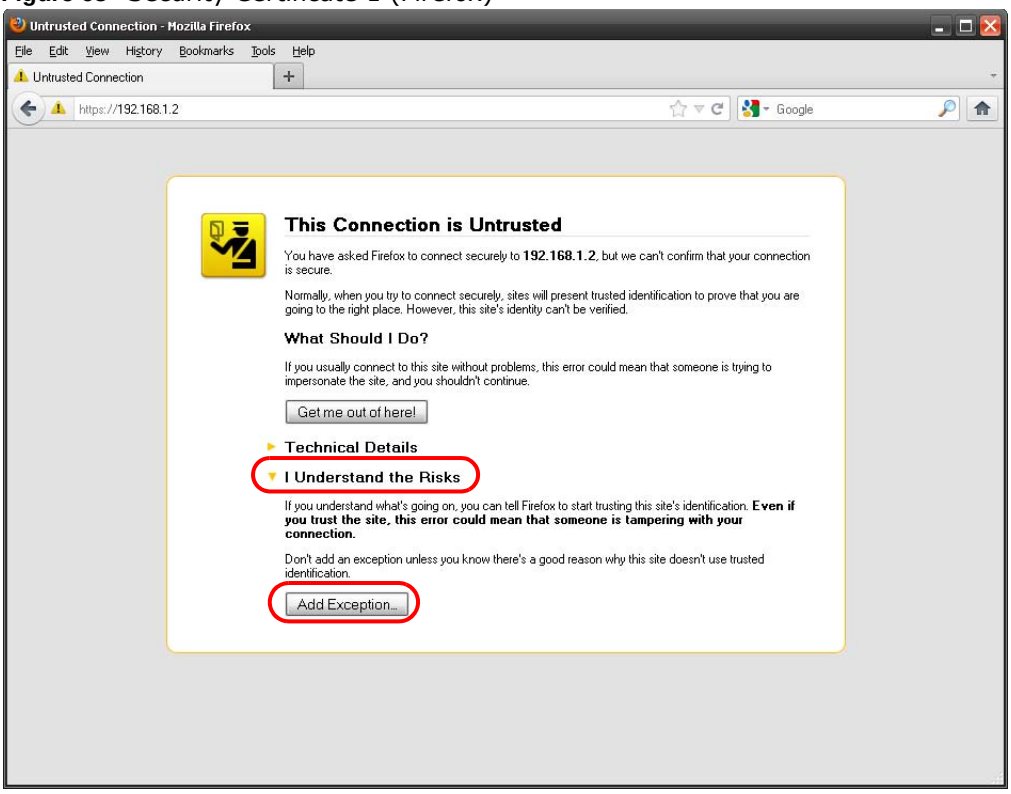
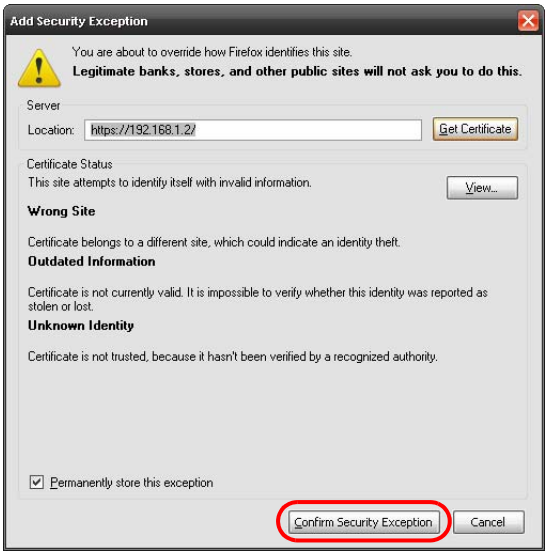

Untrusted Connection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Untrusted Connection
https://192.168.1.2
Google
This Connection is Untrusted
You have asked Firefox to connect securely to 192.168.1.2, but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
I Understand the Risks
If you understand what's going on, you can tell Firefox to start trusting this site's identification. Even if you trust the site, this error could mean that someone is tampering with your connection.
Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.
Add Exception...

Figure 69 Security Certificate 2 (Firefox)


Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location: https://192.168.1.2/
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Wrong Site
Certificate belongs to a different site, which could indicate an identity theft.
Outdated Information
Certificate is not currently valid. It is impossible to verify whether this identity was reported as stolen or lost.
Unknown Identity
Certificate is not trusted, because it hasn't been verified by a recognized authority.
Permanently store this exception
Confirm Security Exception
Cancel

11.4.5.3 Avoiding Browser Warning Messages

Here are the main reasons your browser displays warnings about the NWA's HTTPS server certificate and what you can do to avoid seeing the warnings:

- The issuing certificate authority of the NWA's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the NWA's factory default certificate is the NWA itself since the certificate is a self-signed certificate.

- For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
- To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate. Refer to Appendix A on page 177 for details.

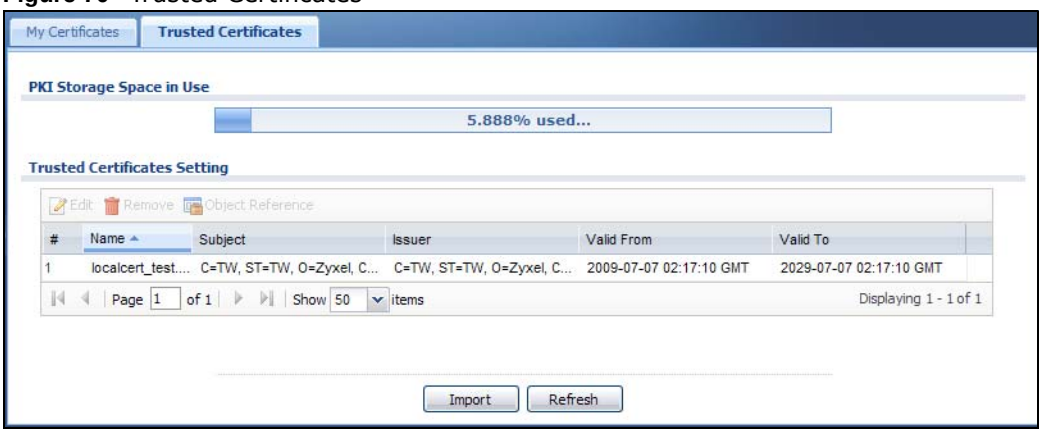
11.4.5.4 Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the NWA.

You must have imported at least one trusted CA to the NWA in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the NWA (see the NWA's **Trusted Certificates** Web Configurator screen).

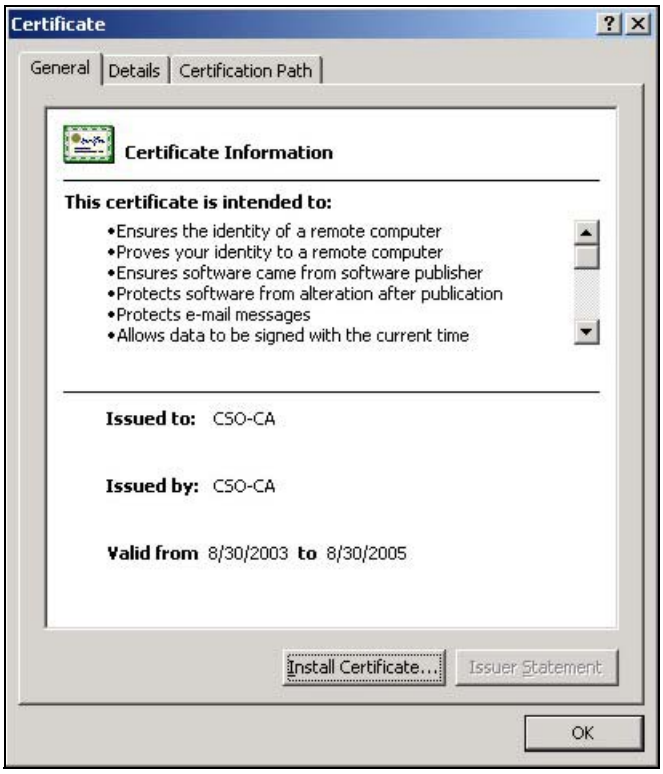
Figure 70 Trusted Certificates



The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

11.4.5.5 Installing the CA's Certificate

1 Double click the CA's trusted certificate to produce a screen similar to the one shown next.



2 Click **Install Certificate** and follow the wizard as shown earlier in this appendix.

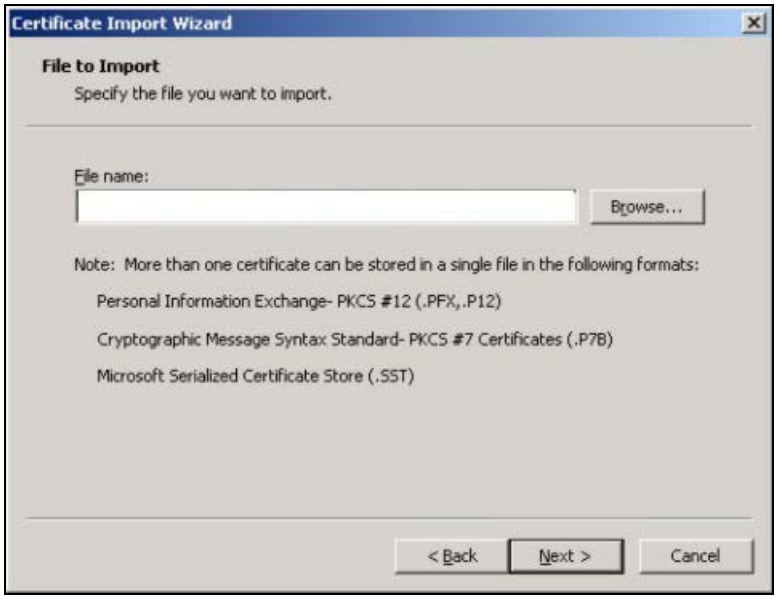
11.4.5.6 Installing a Personal Certificate

You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

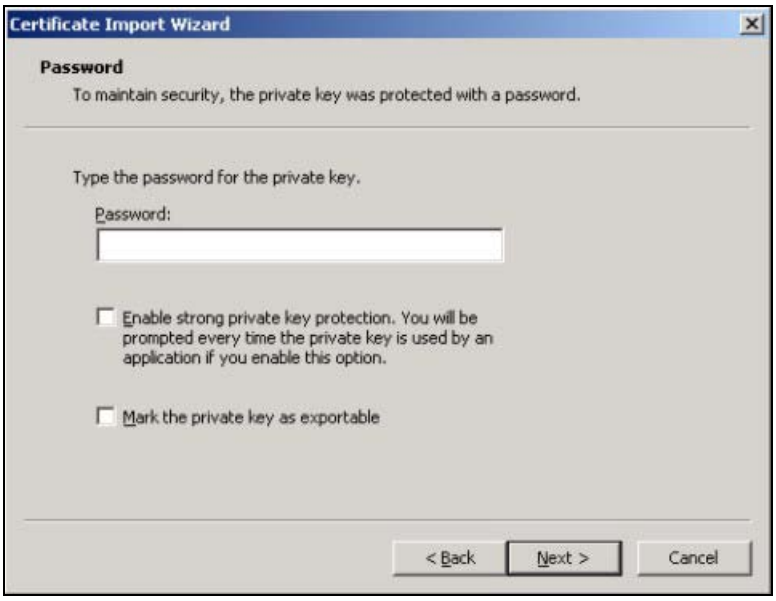
1 Click **Next** to begin the wizard.

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

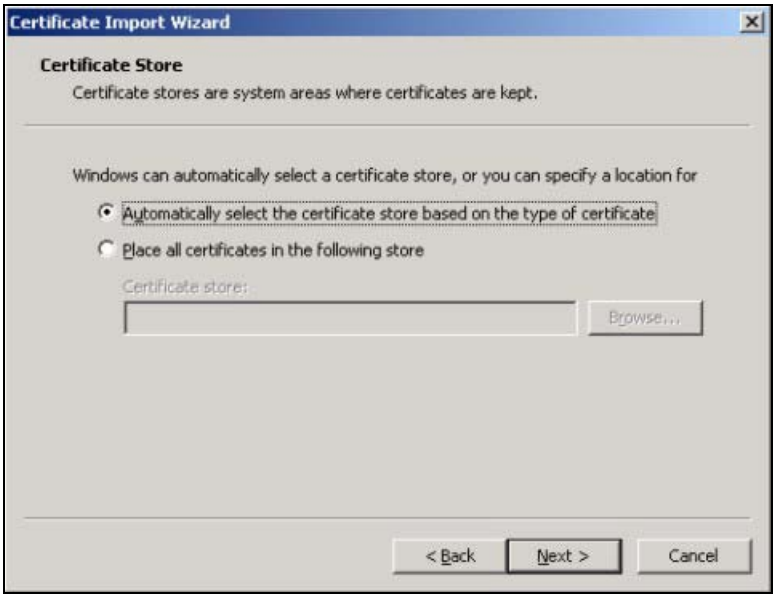
2 The file name and path of the certificate you double-clicked should automatically appear in the **File name** text box. Click **Browse** if you wish to import a different certificate.


Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
Browse...
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
< Back
Next >
Cancel

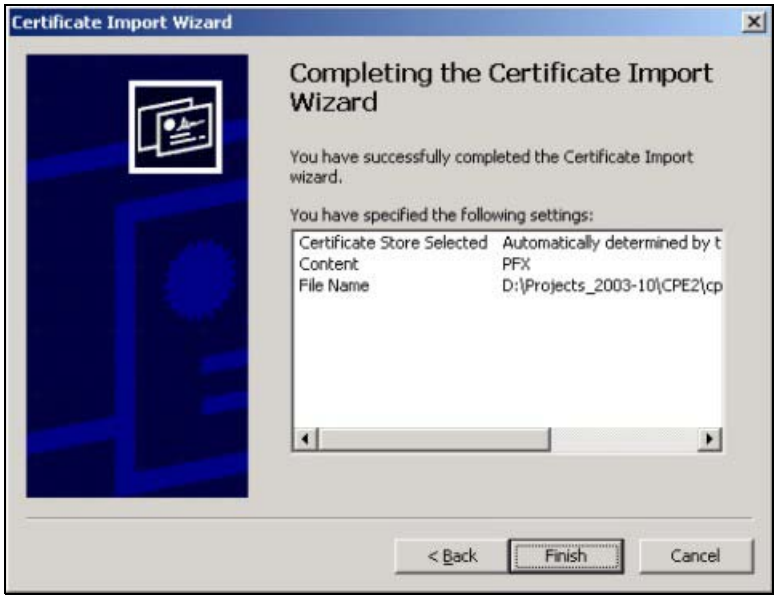
3 Enter the password given to you by the CA.


Certificate Import Wizard
Password
To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
Mark the private key as exportable
< Back
Next >
Cancel

4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

5 Click **Finish** to complete the wizard and begin the import process.



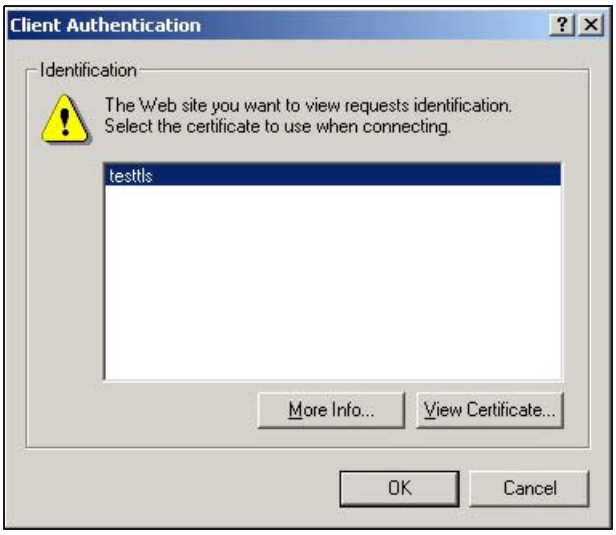
6 You should see the following screen when the certificate is correctly installed on your computer.

11.4.5.7 Using a Certificate When Accessing the NWA

To access the NWA via HTTPS:

1 Enter 'https://NWA IP Address/ in your browser's web address field.

2 When **Authenticate Client Certificates** is selected on the NWA, the following screen asks you to select a personal certificate to send to the NWA. This screen displays even if you only have a single certificate as in the example.



3 You next see the Web Configurator login screen.

11.5 SSH

You can use SSH (Secure SHell) to securely access the NWA's command line interface.

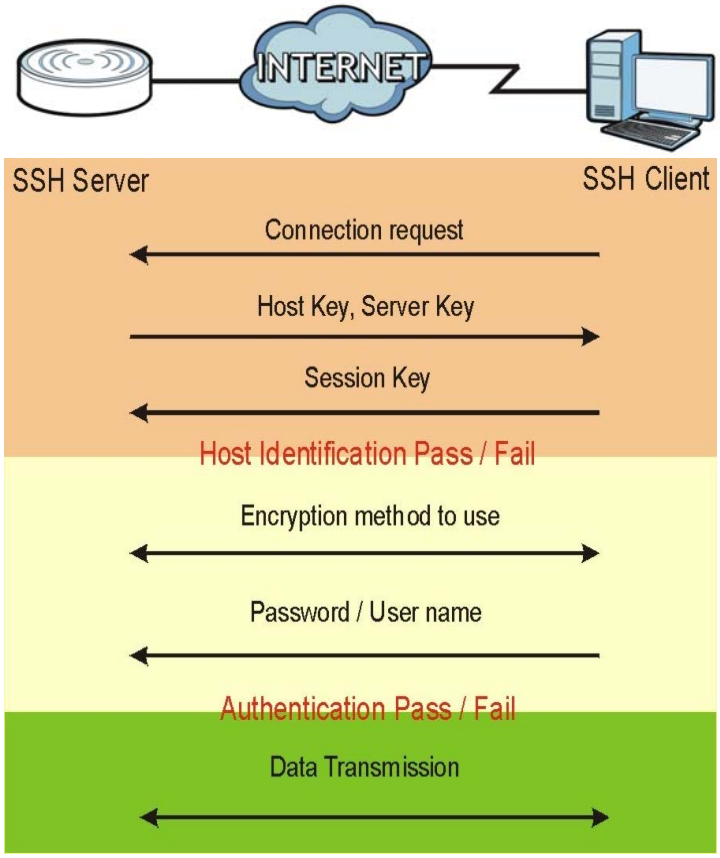
SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. In the following figure, computer B on the Internet uses SSH to securely connect to the NWA (A) for a management session.

Figure 71 SSH Communication Over the WAN Example

11.5.1 How SSH Works

The following figure is an example of how a secure connection is established between two remote hosts using SSH v1.

Figure 72 How SSH v1 Works Example



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

11.5.2 SSH Implementation on the NWA

Your NWA supports SSH versions 1 and 2 using RSA authentication and four encryption methods (AES, 3DES, Archfour, and Blowfish). The SSH server is implemented on the NWA for management using port 22 (by default).

11.5.3 Requirements for Using SSH

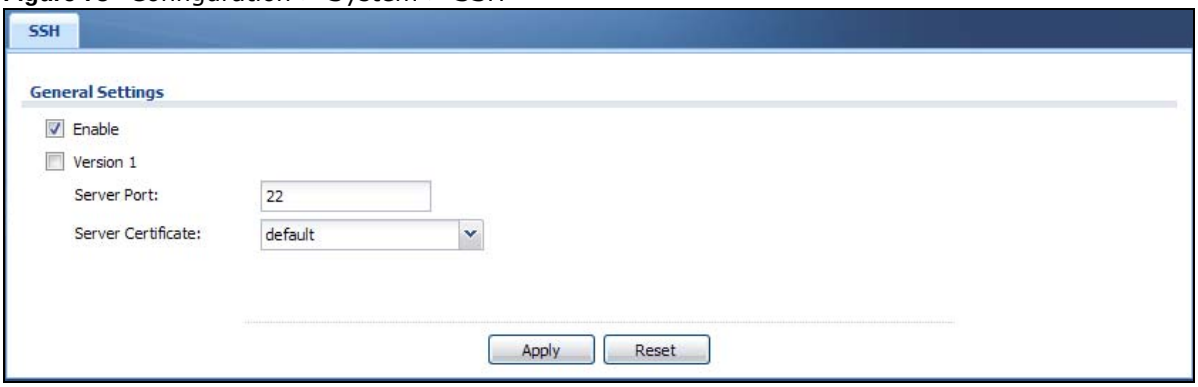
You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the NWA over SSH.

11.5.4 Configuring SSH

Click **Configuration > System > SSH** to open the following screen. Use this screen to configure your NWA's Secure Shell settings.

Note: It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

Figure 73 Configuration > System > SSH



The following table describes the labels in this screen.

Table 57 Configuration > System > SSH

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the NWA CLI using this service.
Version 1	Select the check box to have the NWA use both SSH version 1 and version 2 protocols. If you clear the check box, the NWA uses only SSH version 2 protocol.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the NWA for SSH connections. You must have certificates already configured in the **My Certificates** screen.
Apply	Click **Apply** to save your changes back to the NWA.
Reset	Click **Reset** to return the screen to its last-saved settings.

11.5.5 Examples of Secure Telnet Using SSH

This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the NWA. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

11.5.5.1 Example 1: Microsoft Windows

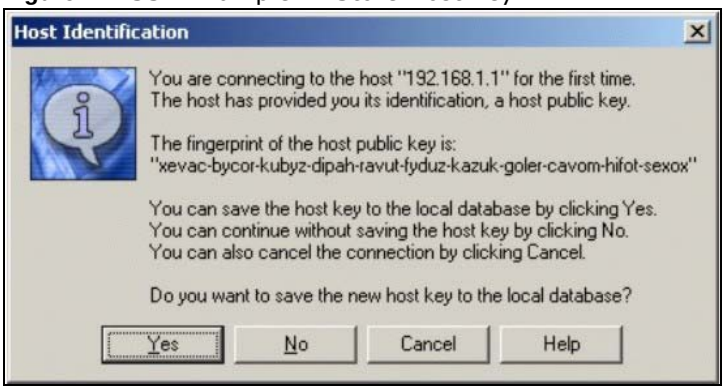
This section describes how to access the NWA using the Secure Shell Client program.

1 Launch the SSH client and specify the connection information (IP address, port number) for the NWA.

2 Configure the SSH client to accept connection using SSH version 1.

3 A window displays prompting you to store the host key in you computer. Click **Yes** to continue.

Figure 74 SSH Example 1: Store Host Key


Host Identification
You are connecting to the host "192.168.1.1" for the first time.
The host has provided you its identification, a host public key.
The fingerprint of the host public key is:
"xevac-bycor-kubyz-dipah-ravut-fyduz-kazuk-goler-cavom-hifot-sexox"
You can save the host key to the local database by clicking Yes.
You can continue without saving the host key by clicking No.
You can also cancel the connection by clicking Cancel.
Do you want to save the new host key to the local database?
Yes
No
Cancel
Help

Enter the password to log in to the NWA. The CLI screen displays next.

11.5.5.2 Example 2: Linux

This section describes how to access the NWA using the OpenSSH client program that comes with most Linux distributions.

1 Test whether the SSH service is available on the NWA.

Enter "`telnet 192.168.1.2 22`" at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the NWA (using the default IP address of 192.168.1.2).

A message displays indicating the SSH protocol version supported by the NWA.

Figure 75 SSH Example 2: Test

```
$ telnet 192.168.1.2 22
Trying 192.168.1.2...
Connected to 192.168.1.2.
Escape character is '^]'.
SSH-1.5-1.0.0
```

2 Enter "ssh –1 192.168.1.2". This command forces your computer to connect to the NWA using SSH version 1. If this is the first time you are connecting to the NWA using SSH, a message displays prompting you to save the host information of the NWA. Type "yes" and press [ENTER].

Then enter the password to log in to the NWA.

Figure 76 SSH Example 2: Log in

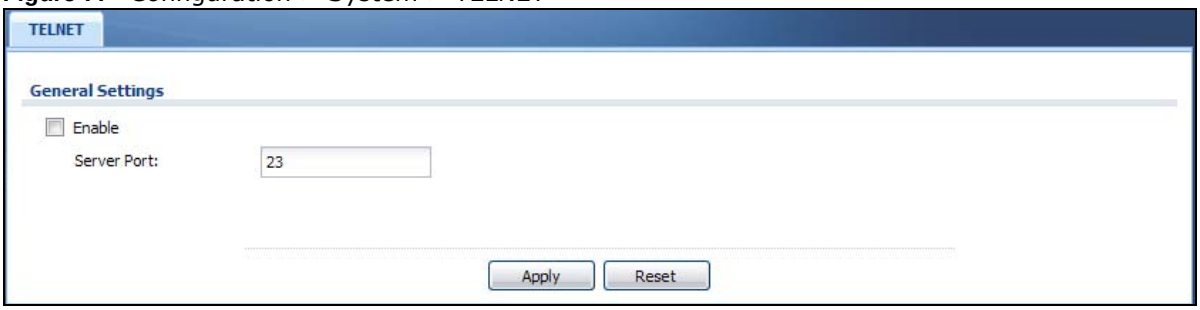
```
$ ssh –1 192.168.1.2
The authenticity of host '192.168.1.2 (192.168.1.2)' can't be established.
RSA1 key fingerprint is 21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.2' (RSA1) to the list of known hosts.
Administrator@192.168.1.2's password:
```

3 The CLI screen displays next.

11.6 Telnet

You can use Telnet to access the NWA's command line interface. Click **Configuration > System > TELNET** to configure your NWA for remote Telnet access. Use this screen to enable or disable Telnet and set the server port number.

Figure 77 Configuration > System > TELNET



The following table describes the labels in this screen.

Table 58 Configuration > System > TELNET

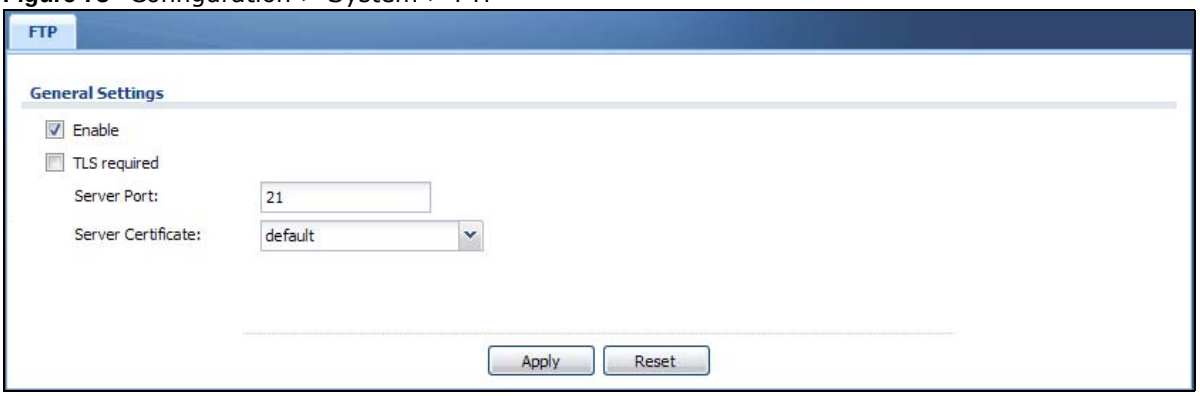
LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the NWA CLI using this service.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Apply	Click **Apply** to save your changes back to the NWA.
Reset	Click **Reset** to return the screen to its last-saved settings.

11.7 FTP

You can upload and download the NWA's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client. See Chapter 13 on page 151 for more information about firmware and configuration files.

To change your NWA's FTP settings, click **Configuration > System > FTP** tab. The screen appears as shown. Use this screen to specify FTP settings.

Figure 78 Configuration > System > FTP



The following table describes the labels in this screen.

Table 59 Configuration > System > FTP

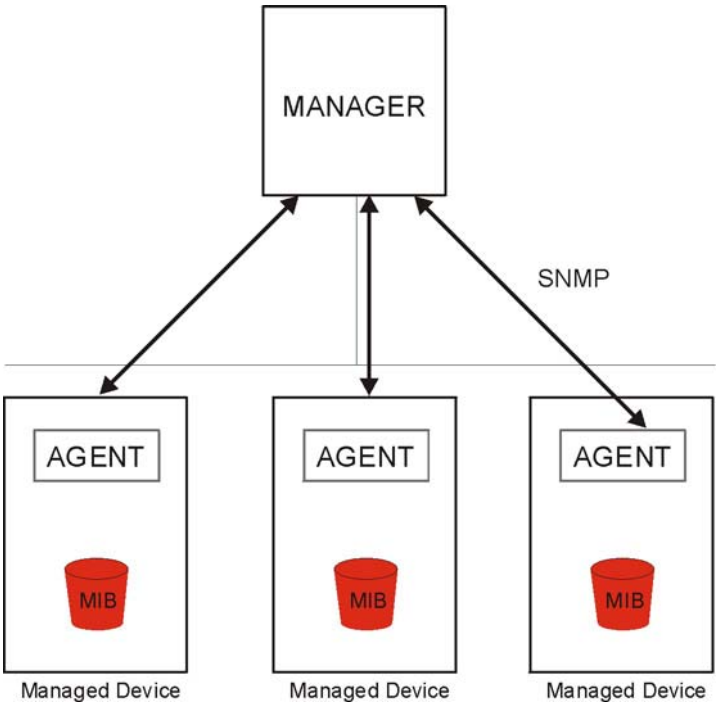
LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the NWA using this service.
TLS required	Select the check box to use FTP over TLS (Transport Layer Security) to encrypt communication. This implements TLS as a security mechanism to secure FTP clients and/or servers.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the NWA for FTP connections. You must have certificates already configured in the **My Certificates** screen.
Apply	Click **Apply** to save your changes back to the NWA.
Reset	Click **Reset** to return the screen to its last-saved settings.

11.8 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your NWA supports SNMP agent functionality, which allows a manager station to manage and monitor the NWA through the network. The NWA supports SNMP version one

(SNMPv1), version two (SNMPv2c), and version three (SNMPv3). The next figure illustrates an SNMP management operation.

Figure 79 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the NWA). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

11.8.1 Supported MIBs

The NWA supports MIB II that is defined in RFC-1213 and RFC-1215. The NWA also supports private MIBs (ZYXEL-ES-CAPWAP.MIB, ZYXEL-ES-COMMON.MIB, ZYXEL-ES-HYBRIDAP.MIB, ZYXEL-ES-PROWLAN.MIB, ZYXEL-ES-RFMGMT.MIB, ZYXEL-ES-SMI.MIB, and ZYXEL-ES-WIRELESS.MIB) to collect information about CPU and memory usage and VPN total throughput. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance. You can download the NWA's MIBs from www.zyxel.com.

11.8.2 SNMP Traps

The NWA will send traps to the SNMP manager when any one of the following events occurs.

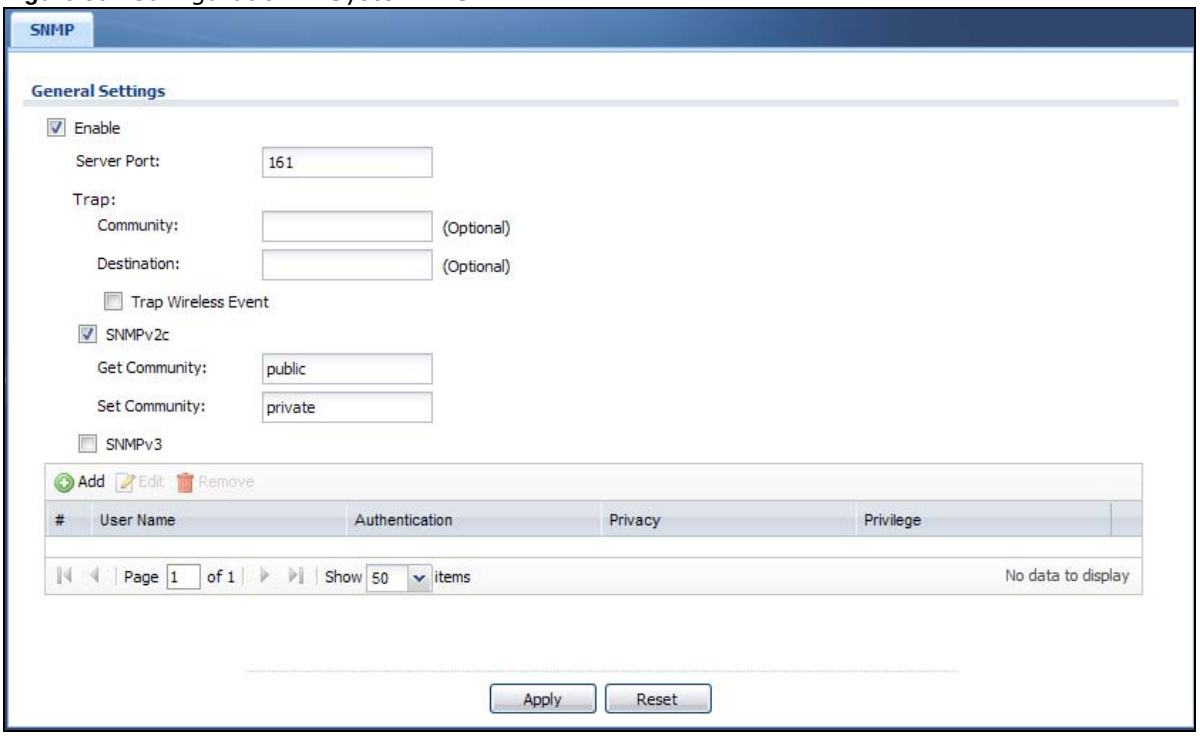
Table 60 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the NWA is turned on or an agent restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.

11.8.3 Configuring SNMP

To change your NWA's SNMP settings, click **Configuration > System > SNMP** tab. The screen appears as shown. Use this screen to configure your SNMP settings. You can also configure user profiles that define allowed SNMPv3 access.

Figure 80 Configuration > System > SNMP



The following table describes the labels in this screen.

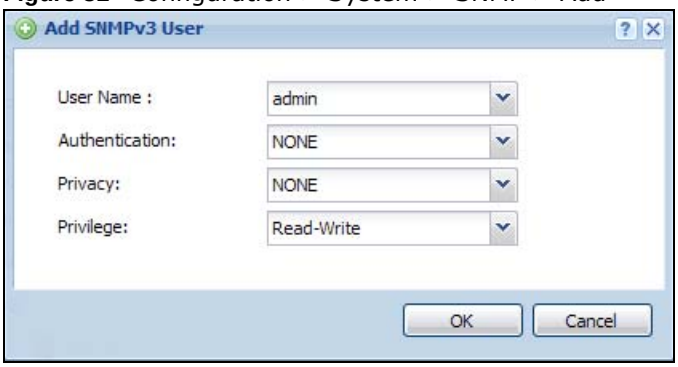
Table 61 Configuration > System > SNMP

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow users to access the NWA using SNMP.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
SNMPv2c	Select this to allow SNMP managers using SNMPv2c to access the NWA.
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is private and allows all requests.
SNMPv3	Select this to allow SNMP managers using SNMPv3 to access the NWA.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The NWA confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This the index number of an SNMPv3 user profile.
User Name	This is the name of the user for which this SNMPv3 user profile is configured.
Authentication	This field displays the type of authentication the SNMPv3 user must use to connect to the NWA using this SNMPv3 user profile.
Privacy	This field displays the type of encryption the SNMPv3 user must use to connect to the NWA using this SNMPv3 user profile.
Privilege	This field displays whether the SNMPv3 user can have read-only or read and write access to the NWA using this SNMPv3 user profile.
Apply	Click **Apply** to save your changes back to the NWA.
Reset	Click **Reset** to return the screen to its last-saved settings.

11.8.4 Adding or Editing an SNMPv3 User Profile

This screen allows you to add or edit an SNMPv3 user profile. To access this screen, click the **Configuration > System > SNMP** screen's **Add** button or select a SNMPv3 user profile from the list and click the **Edit** button.

Figure 81 Configuration > System > SNMP > Add



The following table describes the labels in this screen.

Table 62 Configuration > System > SNMP

LABEL	DESCRIPTION
User Name	Select the user name of the user account for which this SNMPv3 user profile is configured.
Authentication	Select the type of authentication the SNMPv3 user must use to connect to the NWA using this SNMPv3 user profile. Select **NONE** to not authenticate the SNMPv3 user. Select **MD5** to require the SNMPv3 user's password be encrypted by MD5 for authentication. Select **SHA** to require the SNMPv3 user's password be encrypted by SHA for authentication.
Privacy	Select the type of encryption the SNMPv3 user must use to connect to the NWA using this SNMPv3 user profile. Select **NONE** to not encrypt the SNMPv3 communications. Select **DES** to use DES to encrypt the SNMPv3 communications. Select **AES** to use AES to encrypt the SNMPv3 communications.
Privilege	Select whether the SNMPv3 user can have read-only or read and write access to the NWA using this SNMPv3 user profile.
OK	Click **OK** to save your changes back to the NWA.
Cancel	Click **Cancel** to exit this screen without saving your changes.

12

Log and Report

12.1 Overview

Use the system screens to configure daily reporting and log settings.

12.1.1 What You Can Do In this Chapter

- The **Email Daily Report** screen (Section 12.2 on page 139) configures how and where to send daily reports and what reports to send.
- The **Log Setting** screens (Section 12.3 on page 141) specify which logs are e-mailed, where they are e-mailed, and how often they are e-mailed.

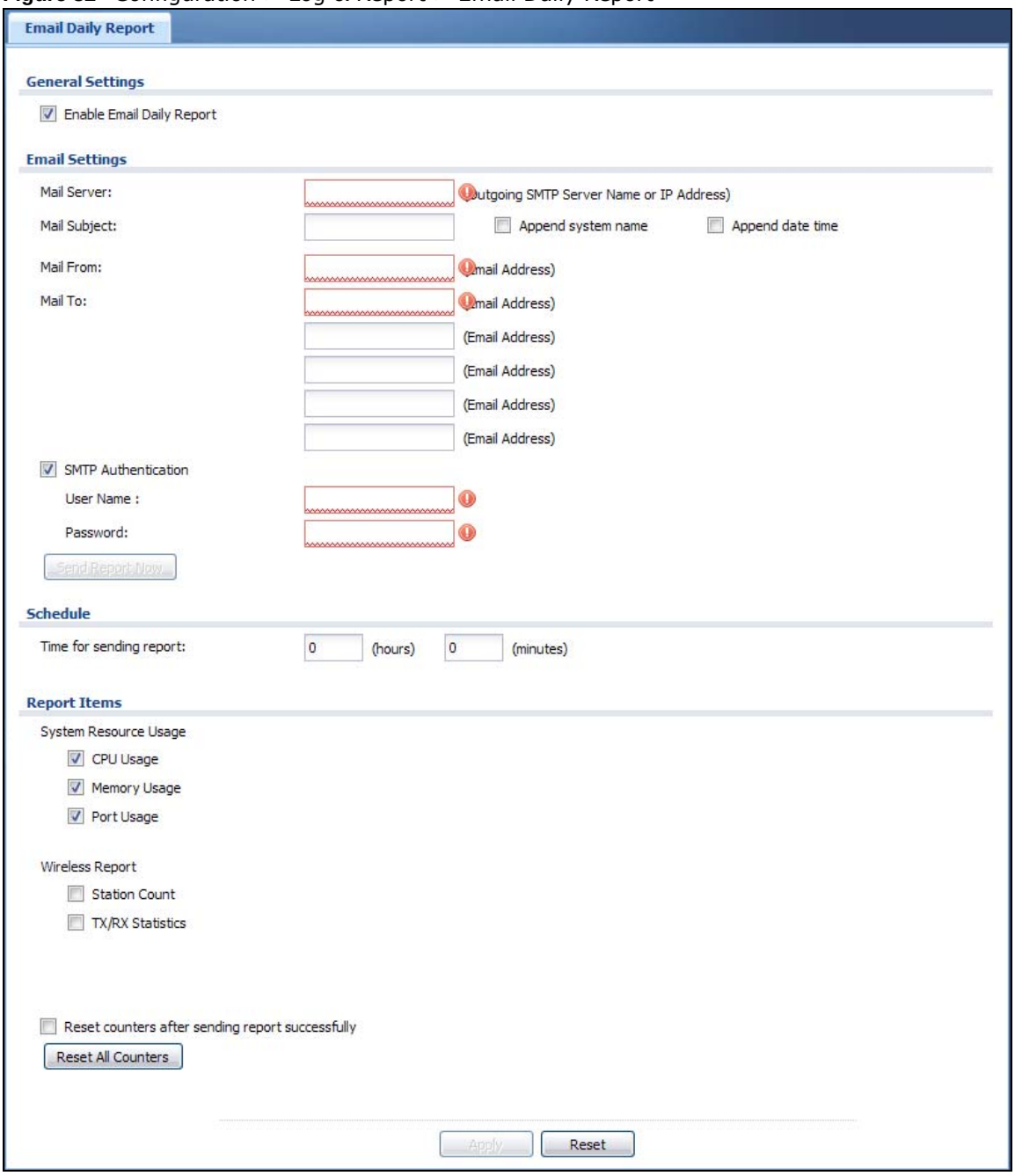
12.2 Email Daily Report

Use this screen to start or stop data collection and view various statistics about traffic passing through your NWA.

Note: Data collection may decrease the NWA's traffic throughput rate.

Click **Configuration > Log & Report > Email Daily Report** to display the following screen. Configure this screen to have the NWA e-mail you system statistics every day.

Figure 82 Configuration > Log & Report > Email Daily Report



The following table describes the labels in this screen.

Table 63 Configuration > Log & Report > Email Daily Report

LABEL	DESCRIPTION
Enable Email Daily Report	Select this to send reports by e-mail every day.
Mail Server	Type the name or IP address of the outgoing SMTP server.

Table 63 Configuration > Log & Report > Email Daily Report (continued)

LABEL	DESCRIPTION
Mail Subject	Type the subject line for the outgoing e-mail. Select **Append system name** to add the NWA's system name to the subject. Select **Append date time** to add the NWA's system date and time to the subject.
Mail From	Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies.
Mail To	Type the e-mail address (or addresses) to which the outgoing e-mail is delivered.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the **SMTP Authentication** check box. Type the user name to provide to the SMTP server when the log is e-mailed.
Password	This box is effective when you select the **SMTP Authentication** check box. Type the password to provide to the SMTP server when the log is e-mailed.
Send Report Now	Click this button to have the NWA send the daily e-mail report immediately.
Time for sending report	Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.
Report Items	Select the information to include in the report. Select **Reset counters after sending report successfully** if you only want to see statistics for a 24 hour period.
Reset All Counters	Click this to discard all report data and start all of the counters over at zero.
Apply	Click **Apply** to save your changes back to the NWA.
Reset	Click **Reset** to return the screen to its last-saved settings.

12.3 Log Setting

These screens control log messages and alerts. A log message stores the information for viewing (for example, in the **Monitor > View Log** screen) or regular e-mailing later, and an alert is e-mailed immediately. Usually, alerts are used for events that require more serious attention, such as system errors and attacks.

The NWA provides a system log and supports e-mail profiles and remote syslog servers. The system log is available on the **View Log** screen, the e-mail profiles are used to mail log messages to the specified destinations, and the other four logs are stored on specified syslog servers.

The **Log Setting** tab also controls what information is saved in each log. For the system log, you can also specify which log messages are e-mailed, where they are e-mailed, and how often they are e-mailed.

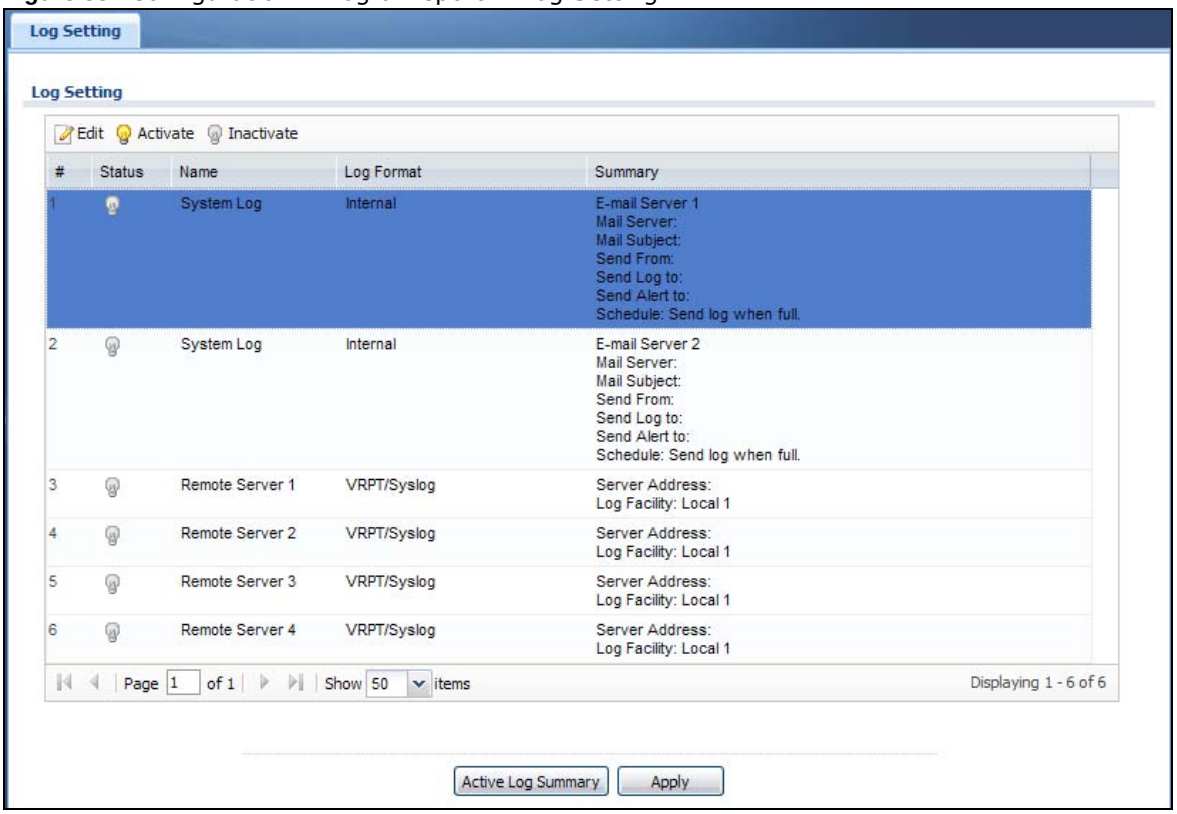
For alerts, the **Log Setting** screen controls which events generate alerts and where alerts are e-mailed.

The **Log Setting** screen provides a summary of all the settings. You can use the **Edit Log Setting** screen to maintain the detailed settings (such as log categories, e-mail addresses, server names, etc.) for any log. Alternatively, if you want to edit what events is included in each log, you can also use the **Active Log Summary** screen to edit this information for all logs at the same time.

12.3.1 Log Setting

To access this screen, click **Configuration > Log & Report > Log Setting**.

Figure 83 Configuration > Log & Report > Log Setting


Log Setting
Log Setting
Edit
Activate
Inactivate
Status Name Log Format Summary
1 System Log Internal E-mail Server 1 Mail Server: Mail Subject: Send From: Send Log to: Send Alert to: Schedule: Send log when full.
2 System Log Internal E-mail Server 2 Mail Server: Mail Subject: Send From: Send Log to: Send Alert to: Schedule: Send log when full.
3 Remote Server 1 VRPT/Syslog Server Address: Log Facility: Local 1
4 Remote Server 2 VRPT/Syslog Server Address: Log Facility: Local 1
5 Remote Server 3 VRPT/Syslog Server Address: Log Facility: Local 1
6 Remote Server 4 VRPT/Syslog Server Address: Log Facility: Local 1
Page 1 of 1
Show 50 items
Displaying 1 - 6 of 6
Active Log Summary
Apply

The following table describes the labels in this screen.

Table 64 Configuration > Log & Report > Log Setting

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This field is a sequential value, and it is not associated with a specific log.
Status	This field shows whether the log is active or not.
Name	This field displays the name of the log (system log or one of the remote servers).
Log Format	This field displays the format of the log. **Internal** - system log; you can view the log on the **View Log** tab. **VRPT/Syslog** - ZyXEL's Vantage Report, syslog-compatible format. **CEF/Syslog** - Common Event Format, syslog-compatible format.
Summary	This field is a summary of the settings for each log.

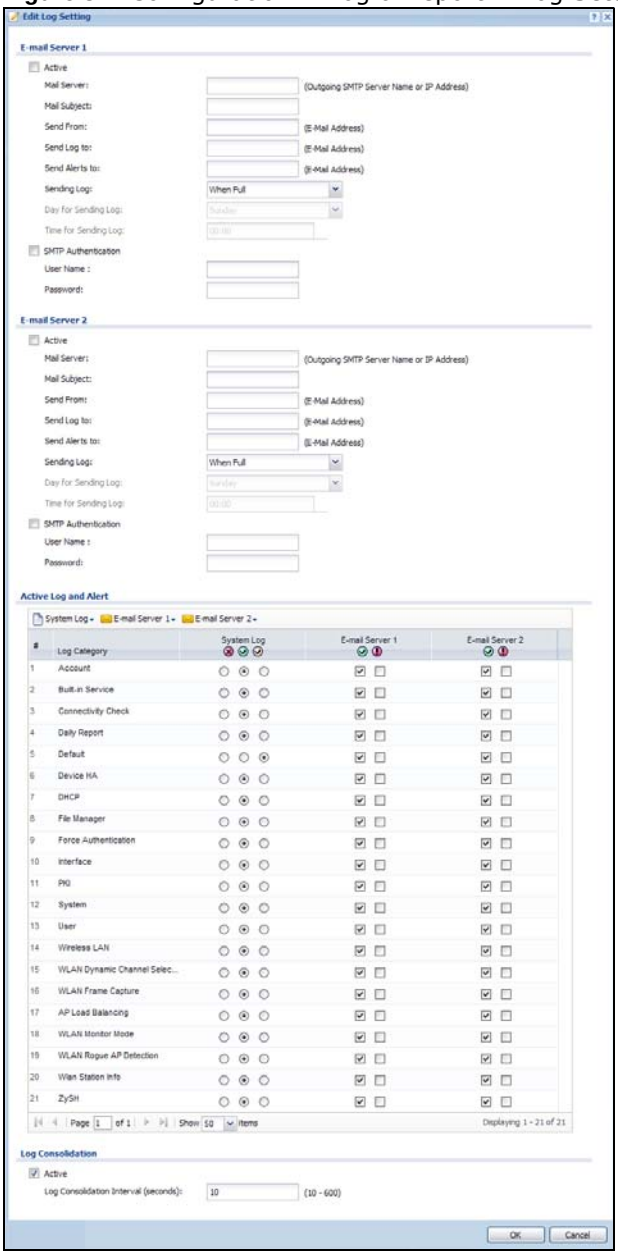
Table 64 Configuration > Log & Report > Log Setting (continued)

LABEL	DESCRIPTION
Active Log Summary	Click this button to open the **Active Log Summary** screen.
Apply	Click this button to save your changes (activate and deactivate logs) and make them take effect.

12.3.2 Edit System Log Settings

This screen controls the detailed settings for each log in the system log (which includes the e-mail profiles). Select a system log entry in the **Log Setting** screen and click the **Edit** icon.

Figure 84 Configuration > Log & Report > Log Setting > Edit System Log Setting



The following table describes the labels in this screen.

Table 65 Configuration > Log & Report > Log Setting > Edit System Log Setting

LABEL	DESCRIPTION
E-Mail Server 1/2	
Active	Select this to send log messages and alerts according to the information in this section. You specify what kinds of log messages are included in log information and what kinds of log messages are included in alerts in the **Active Log and Alert** section.
Mail Server	Type the name or IP address of the outgoing SMTP server.
Mail Subject	Type the subject line for the outgoing e-mail.
Send From	Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies.
Send Log To	Type the e-mail address to which the outgoing e-mail is delivered.
Send Alerts To	Type the e-mail address to which alerts are delivered.
Sending Log	Select how often log information is e-mailed. Choices are: **When Full**, **Hourly and When Full**, **Daily and When Full**, and **Weekly and When Full**.
Day for Sending Log	This field is available if the log is e-mailed weekly. Select the day of the week the log is e-mailed.
Time for Sending Log	This field is available if the log is e-mailed weekly or daily. Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the **SMTP Authentication** check box. Type the user name to provide to the SMTP server when the log is e-mailed.
Password	This box is effective when you select the **SMTP Authentication** check box. Type the password to provide to the SMTP server when the log is e-mailed.
Active Log and Alert	
System log	Use the **System Log** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not log any information for any category for the system log or e-mail any logs to e-mail server 1 or 2. **enable normal logs** (green check mark) - create log messages and alerts for all categories for the system log. If e-mail server 1 or 2 also has normal logs enabled, the NWA will e-mail logs to them. **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information for all categories. The NWA does not e-mail debugging information, even if this setting is selected.
E-mail Server 1	Use the **E-Mail Server 1** drop-down list to change the settings for e-mailing logs to e-mail server 1 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 1 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 1. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 1.

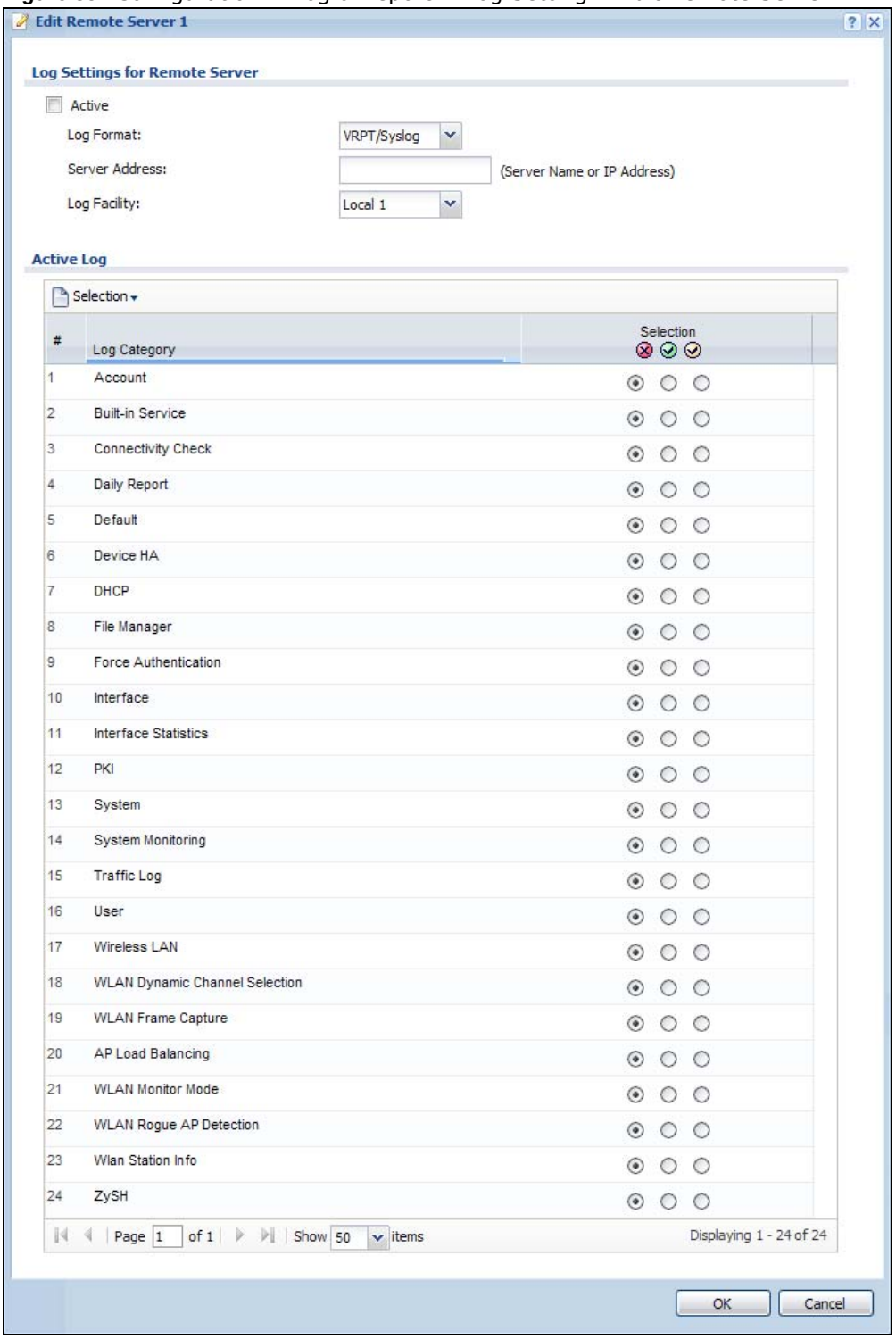
Table 65 Configuration > Log & Report > Log Setting > Edit System Log Setting (continued)

LABEL	DESCRIPTION
E-mail Server 2	Use the **E-Mail Server 2** drop-down list to change the settings for e-mailing logs to e-mail server 2 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 2 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 2. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 2.
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
System log	Select which events you want to log by **Log Category**. There are three choices: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green checkmark) - create log messages and alerts from this category **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information from this category; the NWA does not e-mail debugging information, however, even if this setting is selected.
E-mail Server 1	Select whether each category of events should be included in the log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 1**. The NWA does not e-mail debugging information, even if it is recorded in the **System log**.
E-mail Server 2	Select whether each category of events should be included in log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 2**. The NWA does not e-mail debugging information, even if it is recorded in the **System log**.
Log Consolidation	
Active	Select this to activate log consolidation. Log consolidation aggregates multiple log messages that arrive within the specified **Log Consolidation Interval**. In the **View Log** tab, the text "[count=*x*]", where *x* is the number of original log messages, is appended at the end of the **Message** field, when multiple log messages were aggregated.
Log Consolidation Interval	Type how often, in seconds, to consolidate log information. If the same log message appears multiple times, it is aggregated into one log message with the text "[count=*x*]", where *x* is the number of original log messages, appended at the end of the **Message** field.
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

12.3.3 Edit Remote Server

This screen controls the settings for each log in the remote server (syslog). Select a remote server entry in the **Log Setting** screen and click the **Edit** icon.

Figure 85 Configuration > Log & Report > Log Setting > Edit Remote Server



The following table describes the labels in this screen.

Table 66 Configuration > Log & Report > Log Setting > Edit Remote Server

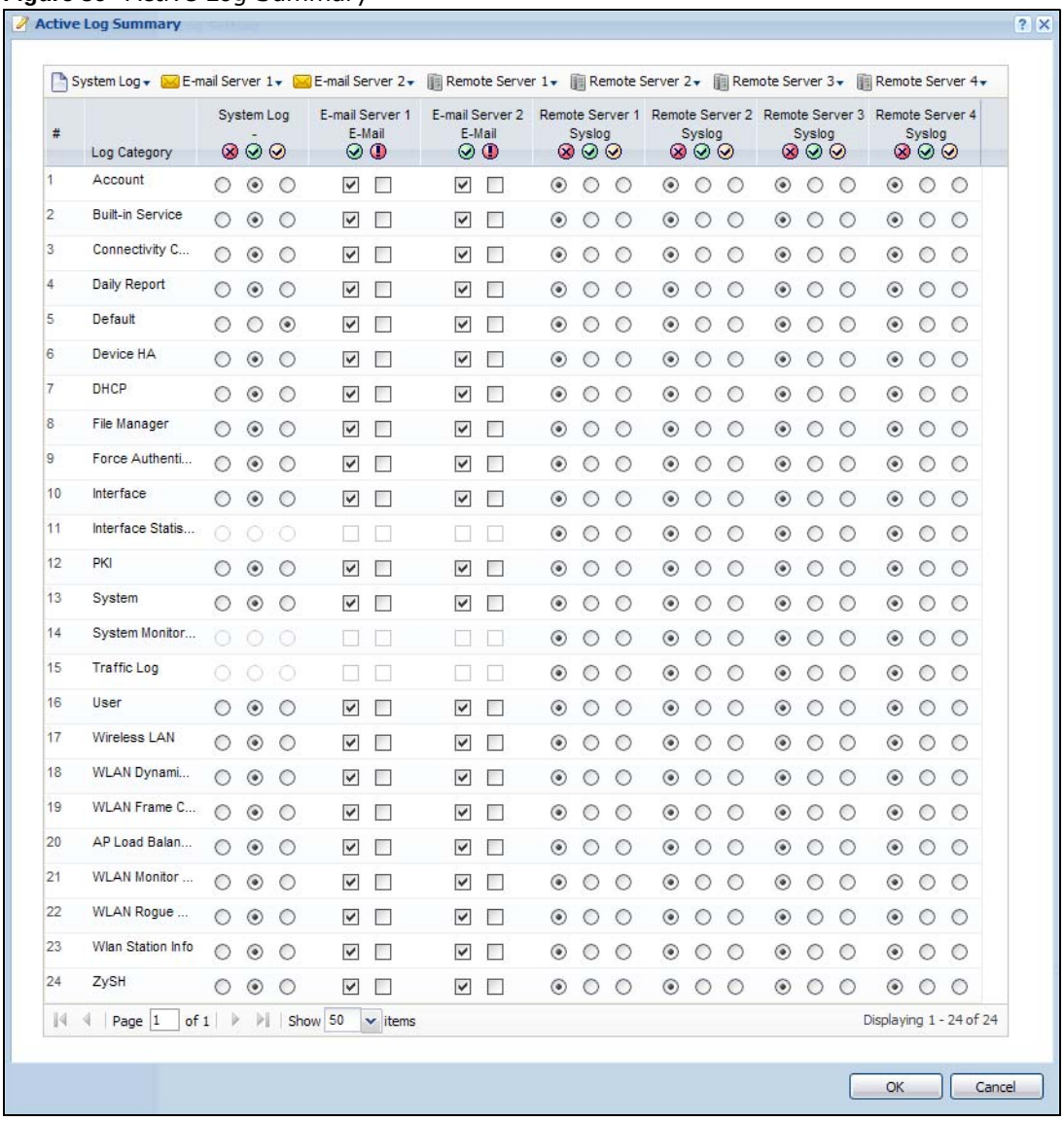
LABEL	DESCRIPTION
Log Settings for Remote Server	
Active	Select this check box to send log information according to the information in this section. You specify what kinds of messages are included in log information in the **Active Log** section.
Log Format	This field displays the format of the log information. It is read-only. **VRPT/Syslog** - ZyXEL's Vantage Report, syslog-compatible format. **CEF/Syslog** - Common Event Format, syslog-compatible format.
Server Address	Type the server name or the IP address of the syslog server to which to send log information.
Log Facility	Select a log facility. The log facility allows you to log the messages to different files in the syslog server. Please see the documentation for your syslog program for more information.
Active Log	
Selection	Use the **Selection** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not send the remote server logs for any log category. **enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories. **enable normal logs and debug logs** (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green checkmark) - log regular information and alerts from this category **enable normal logs and debug logs** (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

12.3.4 Active Log Summary

This screen allows you to view and to edit what information is included in the system log, e-mail profiles, and remote servers at the same time. It does not let you change other log settings (for

example, where and how often log information is e-mailed or remote server names). To access this screen, go to the **Log Setting** screen, and click the **Active Log Summary** button.

Figure 86 Active Log Summary



This screen provides a different view and a different way of indicating which messages are included in each log and each alert. (The **Default** category includes debugging messages generated by open source software.)

The following table describes the fields in this screen.

Table 67 Configuration > Log & Report > Log Setting > Active Log Summary

LABEL	DESCRIPTION
Active Log Summary	If the NWA is set to controller mode, the AC section controls logs generated by the controller and the AP section controls logs generated by the managed APs.
System log	Use the **System Log** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not log any information for any category for the system log or e-mail any logs to e-mail server 1 or 2. **enable normal logs** (green check mark) - create log messages and alerts for all categories for the system log. If e-mail server 1 or 2 also has normal logs enabled, the NWA will e-mail logs to them. **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information for all categories. The NWA does not e-mail debugging information, even if this setting is selected.
E-mail Server 1	Use the **E-Mail Server 1** drop-down list to change the settings for e-mailing logs to e-mail server 1 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 1 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 1. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 1.
E-mail Server 2	Use the **E-Mail Server 2** drop-down list to change the settings for e-mailing logs to e-mail server 2 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 2 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 2. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 2.
Remote Server 1~4	For each remote server, use the **Selection** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not send the remote server logs for any log category. **enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories. **enable normal logs and debug logs** (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
System log	Select which events you want to log by **Log Category**. There are three choices: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green checkmark) - create log messages and alerts from this category **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information from this category; the NWA does not e-mail debugging information, however, even if this setting is selected.

Table 67 Configuration > Log & Report > Log Setting > Active Log Summary (continued)

LABEL	DESCRIPTION
E-mail Server 1 E-mail	Select whether each category of events should be included in the log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 1**. The NWA does not e-mail debugging information, even if it is recorded in the **System log**.
E-mail Server 2 E-mail	Select whether each category of events should be included in log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 2**. The NWA does not e-mail debugging information, even if it is recorded in the **System log**.
Remote Server 1~4 Syslog	For each remote server, select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green checkmark) - log regular information and alerts from this category **enable normal logs and debug logs** (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

13

File Manager

13.1 Overview

Configuration files define the NWA's settings. Shell scripts are files of commands that you can store on the NWA and run when you need them. You can apply a configuration file or run a shell script without the NWA restarting. You can store multiple configuration files and shell script files on the NWA. You can edit configuration files or shell scripts in a text editor and upload them to the NWA. Configuration files use a .conf extension and shell scripts use a .zysh extension.

13.1.1 What You Can Do in this Chapter

- The **Configuration File** screen (Section 13.2 on page 152) stores and names configuration files. You can also download and upload configuration files.
- The **Firmware Package** screen (Section 13.3 on page 157) checks your current firmware version and uploads firmware to the NWA.
- The **Shell Script** screen (Section 13.4 on page 159) stores, names, downloads, uploads and runs shell script files.

13.1.2 What you Need to Know

The following terms and concepts may help as you read this chapter.

Configuration Files and Shell Scripts

When you apply a configuration file, the NWA uses the factory default settings for any features that the configuration file does not include. When you run a shell script, the NWA only applies the commands that it contains. Other settings do not change.

These files have the same syntax, which is also identical to the way you run CLI commands manually. An example is shown below

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
#configure default radio profile, change 2GHz channel to 11 & Tx output power # to
50%
wlan-radio-profile default
2g-channel 11
output-power 50%
exit
write
```

While configuration files and shell scripts have the same syntax, the NWA applies configuration files differently than it runs shell scripts. This is explained below.

Table 68 Configuration Files and Shell Scripts in the NWA

Configuration Files (.conf)	Shell Scripts (.zysh)
• Resets to default configuration. • Goes into CLI **Configuration** mode. • Runs the commands in the configuration file.	• Goes into CLI **Privilege** mode. • Runs the commands in the shell script.

You have to run the aforementioned example as a shell script because the first command is run in **Privilege** mode. If you remove the first command, you have to run the example as a configuration file because the rest of the commands are executed in **Configuration** mode.

Comments in Configuration Files or Shell Scripts

In a configuration file or shell script, use "#" or "!" as the first character of a command line to have the NWA treat the line as a comment.

Your configuration files or shell scripts can use "exit" or a command line consisting of a single "!" to have the NWA exit sub command mode.

Note: "exit" or "!'" must follow sub commands if it is to make the NWA exit sub command mode.

In the following example lines 1 and 2 are comments. Line 5 exits sub command mode.

```
! this is from Joe
# on 2010/12/05
wlan-ssid-profile default
ssid Joe-AP
qos wmm
security default
!
```

Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the NWA processes the file line-by-line. The NWA checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the NWA finds an error, it stops applying the configuration file or shell script and generates a log.

You can change the way a configuration file or shell script is applied. Include `setenv stop-on-error off` in the configuration file or shell script. The NWA ignores any errors in the configuration file or shell script and applies all of the valid commands. The NWA still generates a log for any errors.

13.2 Configuration File

Click **Maintenance > File Manager > Configuration File** to open this screen. Use the **Configuration File** screen to store, run, and name configuration files. You can also download

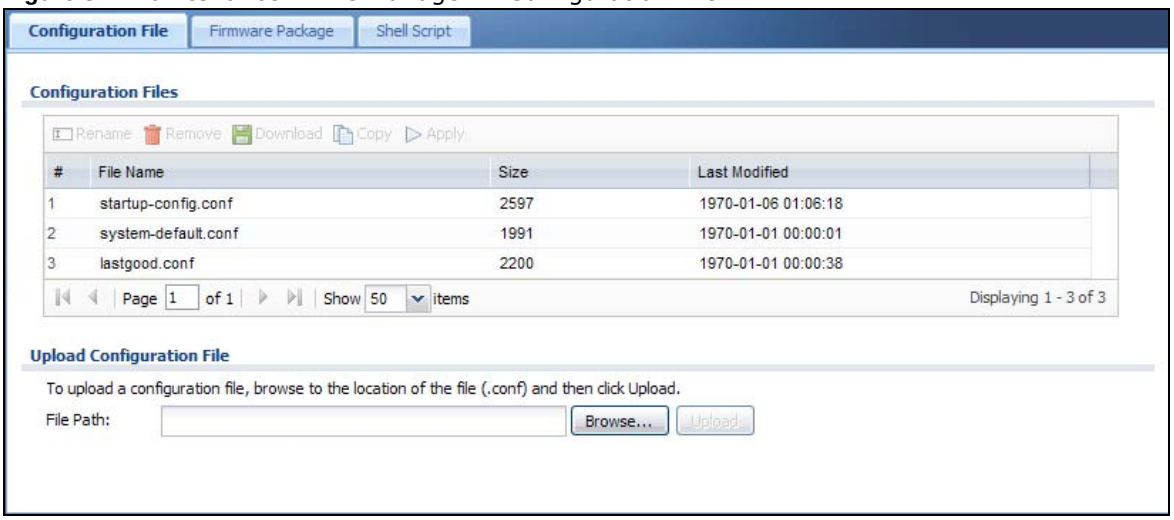
configuration files from the NWA to your computer and upload configuration files from your computer to the NWA.

Once your NWA is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Configuration File Flow at Restart

- If there is not a **startup-config.conf** when you restart the NWA (whether through a management interface or by physically turning the power off and back on), the NWA uses the **system-default.conf** configuration file with the NWA's default settings.
- If there is a **startup-config.conf**, the NWA checks it for errors and applies it. If there are no errors, the NWA uses it and copies it to the **lastgood.conf** configuration file as a back up file. If there is an error, the NWA generates a log and copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the NWA applies the **system-default.conf** configuration file.
- You can change the way the **startup-config.conf** file is applied. Include the `setenv-startup stop-on-error off` command. The NWA ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The NWA still generates a log for any errors.

Figure 87 Maintenance > File Manager > Configuration File



Do not turn off the NWA while configuration file upload is in progress.

The following table describes the labels in this screen.

Table 69 Maintenance > File Manager > Configuration File

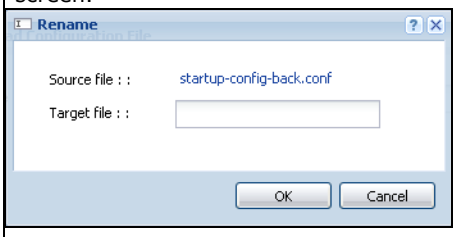
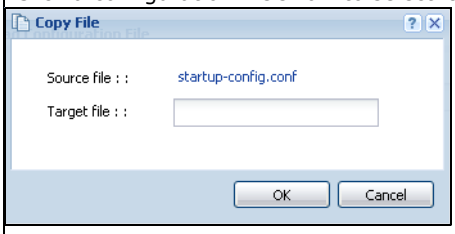
LABEL	DESCRIPTION
Rename	Use this button to change the label of a configuration file on the NWA. You can only rename manually saved configuration files. You cannot rename the **lastgood.conf**, **system-default.conf** and **startup-config.conf** files. You cannot rename a configuration file to the name of another configuration file in the NWA. Click a configuration file's row to select it and click **Rename** to open the **Rename File** screen.  Specify the new name for the configuration file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Remove	Click a configuration file's row to select it and click **Remove** to delete it from the NWA. You can only delete manually saved configuration files. You cannot delete the **system-default.conf**, **startup-config.conf** and **lastgood.conf** files. A pop-up window asks you to confirm that you want to delete the configuration file. Click **OK** to delete the configuration file or click **Cancel** to close the screen without deleting the configuration file.
Download	Click a configuration file's row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a configuration file on the NWA. Click a configuration file's row to select it and click **Copy** to open the **Copy File** screen.  Specify a name for the duplicate configuration file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.

Table 69 Maintenance > File Manager > Configuration File (continued)

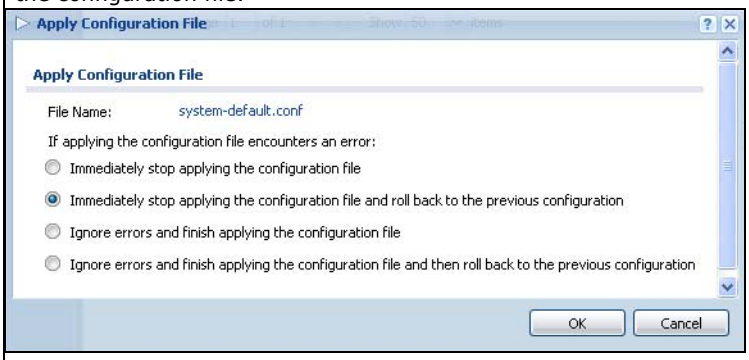
LABEL	DESCRIPTION
Apply	Use this button to have the NWA use a specific configuration file. Click a configuration file's row to select it and click **Apply** to have the NWA use that configuration file. The NWA does not have to restart in order to use a different configuration file, although you will need to wait for a few minutes while the system reconfigures. The following screen gives you options for what the NWA is to do if it encounters an error in the configuration file.  **Immediately stop applying the configuration file** - this is not recommended because it would leave the rest of the configuration blank. If the interfaces were not configured before the first error, the console port may be the only way to access the device. **Immediately stop applying the configuration file and roll back to the previous configuration** - this gets the NWA started with a fully valid configuration file as quickly as possible. **Ignore errors and finish applying the configuration file** - this applies the valid parts of the configuration file and generates error logs for all of the configuration file's errors. This lets the NWA apply most of your configuration and you can refer to the logs for what to fix. **Ignore errors and finish applying the configuration file and then roll back to the previous configuration** - this applies the valid parts of the configuration file, generates error logs for all of the configuration file's errors, and starts the NWA with a fully valid configuration file. Click **OK** to have the NWA start applying the configuration file or click **Cancel** to close the screen
#	This column displays the number for each configuration file entry. This field is a sequential value, and it is not associated with a specific address. The total number of configuration files that you can save depends on the sizes of the configuration files and the available flash storage space.

Table 69 Maintenance > File Manager > Configuration File (continued)

LABEL	DESCRIPTION
File Name	This column displays the label that identifies a configuration file. You cannot delete the following configuration files or change their file names. The **system-default.conf** file contains the NWA's default settings. Select this file and click **Apply** to reset all of the NWA settings to the factory defaults. This configuration file is included when you upload a firmware package. The **startup-config.conf** file is the configuration file that the NWA is currently using. If you make and save changes during your management session, the changes are applied to this configuration file. The NWA applies configuration changes made in the Web Configurator to the configuration file when you click **Apply** or **OK**. It applies configuration changes made via commands when you use the `write` command. The **lastgood.conf** is the most recently used (valid) configuration file that was saved when the device last restarted. If you upload and apply a configuration file with an error, you can apply lastgood.conf to return to a valid configuration.
Size	This column displays the size (in KB) of a configuration file.
Last Modified	This column displays the date and time that the individual configuration files were last changed or saved.
Upload Configuration File	The bottom part of the screen allows you to upload a new or previously saved configuration file from your computer to your NWA You cannot upload a configuration file named **system-default.conf** or **lastgood.conf**. If you upload **startup-config.conf**, it will replace the current configuration and immediately apply the new settings.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .conf file you want to upload. The configuration file must use a ".conf" filename extension. You will receive an error message if you try to upload a fie of a different format. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

13.2.1 Example of Configuration File Download Using FTP

The following example gets a configuration file named startup-config.conf from the NWA and saves it on the computer.

1. Connect your computer to the NWA.
2. The FTP server IP address of the NWA in standalone AP mode is 192.168.1.2, so set your computer to use a static IP address from 192.168.1.3 ~192.168.1.254.
3. Use an FTP client on your computer to connect to the NWA. For example, in the Windows command prompt, type `ftp 192.168.1.2`. Keep the console session connected in order to see when the firmware recovery finishes.
4. Enter your user name when prompted.
5. Enter your password as requested.
6. Use "cd" to change to the directory that contains the files you want to download.
7. Use "dir" or "ls" if you need to display a list of the files in the directory.

8 Use "get" to download files. Transfer the configuration file on the NWA to your computer. Type `get` followed by the name of the configuration file. This examples uses `get startup-config.conf`.

```
C:\>ftp 192.168.1.2
Connected to 192.168.1.2.
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 5 allowed.
220-Local time is now 21:28. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 600 minutes of inactivity.
User (192.168.1.2:(none)): admin
331 User admin OK. Password required
Password:
230 OK. Current restricted directory is /
ftp> cd conf
250 OK. Current directory is /conf
ftp> ls
200 PORT command successful
150 Connecting to port 5001
lastgood.conf
startup-config.conf
system-default.conf
226 3 matches total
ftp: 57 bytes received in 0.33Seconds 0.17Kbytes/sec.
ftp> get startup-config.conf
200 PORT command successful
150 Connecting to port 5002
226-File successfully transferred
226 0.002 seconds (measured here), 1.66 Mbytes per second
ftp: 2928 bytes received in 0.02Seconds 183.00Kbytes/sec.
ftp>
```

9 Wait for the file transfer to complete.

10 Enter "quit" to exit the ftp prompt.

13.3 Firmware Package

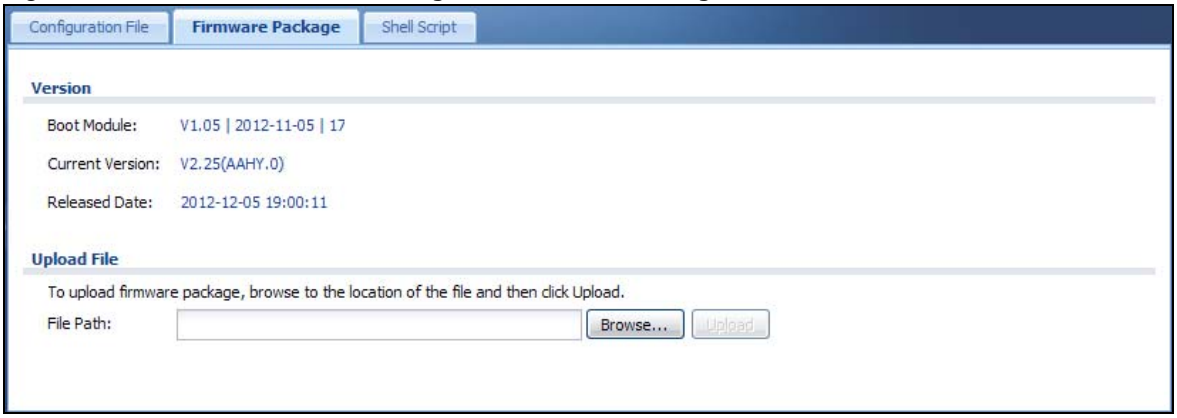
Click **Maintenance > File Manager > Firmware Package** to open this screen. Use the **Firmware Package** screen to check your current firmware version and upload firmware to the NWA.

Note: The Web Configurator is the recommended method for uploading firmware. You only need to use the command line interface if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

Find the firmware package at www.zyxel.com in a file that (usually) uses a .bin extension.

The firmware update can take up to five minutes. Do not turn off or reset the NWA while the firmware update is in progress!

Figure 88 Maintenance > File Manager > Firmware Package



The following table describes the labels in this screen.

Table 70 Maintenance > File Manager > Firmware Package

LABEL	DESCRIPTION
Boot Module	This is the version of the boot module that is currently on the NWA.
Current Version	This is the firmware version and the date created.
Released Date	This is the date that the version of the firmware was created.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the NWA again.

Note: The NWA automatically reboots after a successful upload.

The NWA automatically restarts causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 89 Network Temporarily Disconnected

After five minutes, log in again and check your new firmware version in the **Dashboard** screen.

13.3.1 Example of Firmware Upload Using FTP

This procedure requires the NWA's firmware. Download the firmware package from www.zyxel.com and unzip it. The firmware file uses a .bin extension, for example, "225AAHY0C0.bin". Do the following after you have obtained the firmware file.

1. Connect your computer to the NWA.
2. The FTP server IP address of the NWA in standalone AP mode is 192.168.1.2, so set your computer to use a static IP address from 192.168.1.3 ~192.168.1.254.
3. Use an FTP client on your computer to connect to the NWA. For example, in the Windows command prompt, type `ftp 192.168.1.2`. Keep the console session connected in order to see when the firmware recovery finishes.
4. Enter your user name when prompted.
5. Enter your password as requested.
6. Enter "hash" for FTP to print a `#' character for every 1024 bytes of data you upload so that you can watch the file transfer progress.
7. Enter "bin" to set the transfer mode to binary.
8. Transfer the firmware file from your computer to the NWA. Type `put` followed by the path and name of the firmware file. This examples uses `put C:\ftproot\NWA_FW\225AAHY0C0.bin`.

```
C:\>ftp 192.168.1.2
Connected to 192.168.1.2.
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 5 allowed.
220-Local time is now 21:28. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 600 minutes of inactivity.
User (192.168.1.2:(none)): admin
331 User admin OK. Password required
Password:
230 OK. Current restricted directory is /
ftp> hash
Hash mark printing On  ftp: (2048 bytes/hash mark) .
ftp> bin
200 TYPE is now 8-bit binary
ftp> put C:\ftproot\NWA_FW\225AAHY0C0.bin
```

9. Wait for the file transfer to complete.
10. Enter "quit" to exit the ftp prompt.

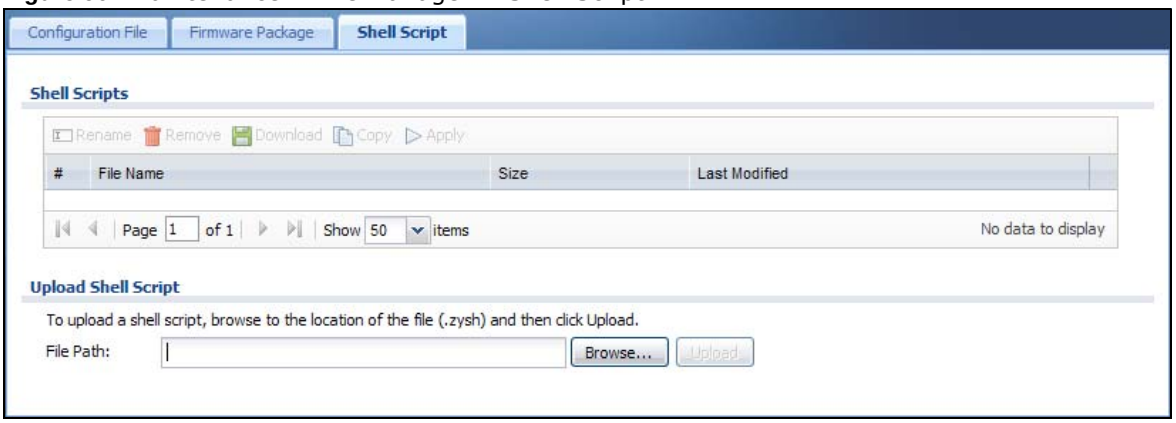
13.4 Shell Script

Use shell script files to have the NWA use commands that you specify. Use a text editor to create the shell script files. They must use a ".zysh" filename extension.

Click **Maintenance > File Manager > Shell Script** to open this screen. Use the **Shell Script** screen to store, name, download, upload and run shell script files. You can store multiple shell script files on the NWA at the same time.

Note: You should include `write` commands in your scripts. If you do not use the `write` command, the changes will be lost when the NWA restarts. You could use multiple `write` commands in a long script.

Figure 90 Maintenance > File Manager > Shell Script



Each field is described in the following table.

Table 71 Maintenance > File Manager > Shell Script

LABEL	DESCRIPTION
Rename	Use this button to change the label of a shell script file on the NWA. You cannot rename a shell script to the name of another shell script in the NWA. Click a shell script's row to select it and click **Rename** to open the **Rename File** screen. Specify the new name for the shell script file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Remove	Click a shell script file's row to select it and click **Delete** to delete the shell script file from the NWA. A pop-up window asks you to confirm that you want to delete the shell script file. Click **OK** to delete the shell script file or click **Cancel** to close the screen without deleting the shell script file.
Download	Click a shell script file's row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a shell script file on the NWA. Click a shell script file's row to select it and click **Copy** to open the **Copy File** screen. Specify a name for the duplicate file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Run	Use this button to have the NWA use a specific shell script file. Click a shell script file's row to select it and click **Run** to have the NWA use that shell script file. You may need to wait awhile for the NWA to finish applying the commands.

Table 71 Maintenance > File Manager > Shell Script (continued)

LABEL	DESCRIPTION
#	This column displays the number for each shell script file entry.
File Name	This column displays the label that identifies a shell script file.
Size	This column displays the size (in KB) of a shell script file.
Last Modified	This column displays the date and time that the individual shell script files were last changed or saved.
Upload Shell Script	The bottom part of the screen allows you to upload a new or previously saved shell script file from your computer to your NWA.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .zysh file you want to upload.
Upload	Click **Upload** to begin the upload process. This process may take up to several minutes.

14 Diagnostics

14.1 Overview

Use the diagnostics screen for troubleshooting.

14.1.1 What You Can Do in this Chapter

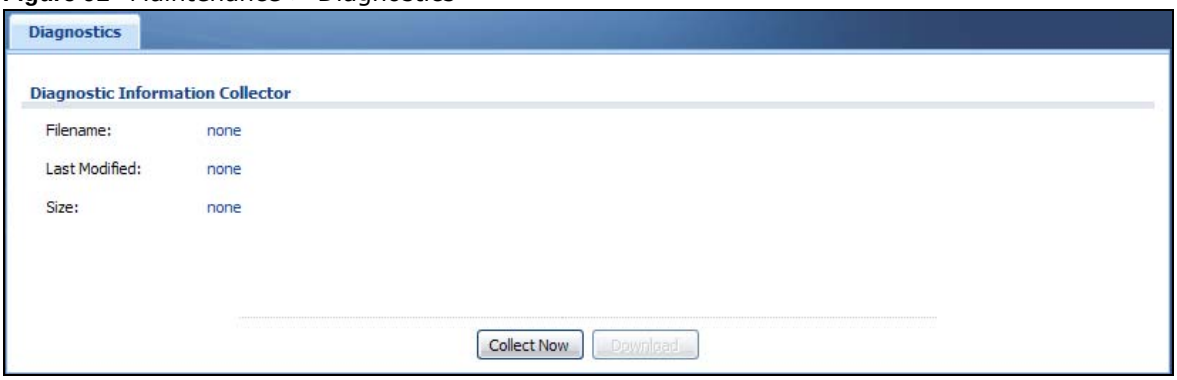
- The **Diagnostics** screen (Section 14.2 on page 163) generates a file containing the NWA's configuration and diagnostic information if you need to provide it to customer support during troubleshooting.

14.2 Diagnostics

This screen provides an easy way for you to generate a file containing the NWA's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting.

Click **Maintenance > Diagnostics** to open the **Diagnostic** screen.

Figure 91 Maintenance > Diagnostics



The following table describes the labels in this screen.

Table 72 Maintenance > Diagnostics

LABEL	DESCRIPTION
Filename	This is the name of the most recently created diagnostic file.
Last modified	This is the date and time that the last diagnostic file was created. The format is yyyy-mm-dd hh:mm:ss.
Size	This is the size of the most recently created diagnostic file.

Table 72 Maintenance > Diagnostics

LABEL	DESCRIPTION
Collect Now	Click this to have the NWA create a new diagnostic file.
Download	Click this to save the most recent diagnostic file to a computer.

15 Reboot

15.1 Overview

Use this to restart the device.

15.1.1 What You Need To Know

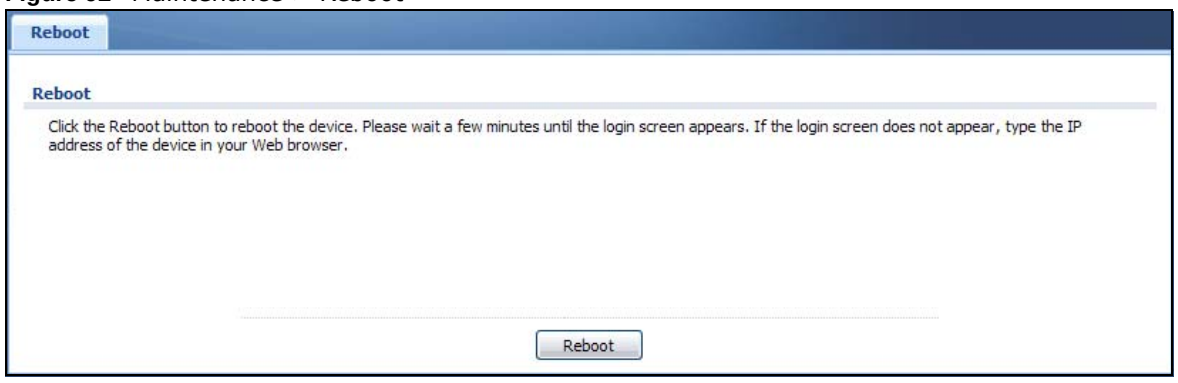
If you applied changes in the Web configurator, these were saved automatically and do not change when you reboot. If you made changes in the CLI, however, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot.

Reboot is different to reset; reset returns the device to its default configuration.

15.2 Reboot

This screen allows remote users can restart the device. To access this screen, click **Maintenance** > **Reboot**.

Figure 92 Maintenance > Reboot


Reboot
Reboot
Click the Reboot button to reboot the device. Please wait a few minutes until the login screen appears. If the login screen does not appear, type the IP address of the device in your Web browser.
Reboot

Click the **Reboot** button to restart the NWA. Wait a few minutes until the login screen appears. If the login screen does not appear, type the IP address of the device in your Web browser.

You can also use the CLI command `reboot` to restart the NWA.

16 Shutdown

16.1 Overview

Use this screen to shutdown the device.

Always use Maintenance > Shutdown > Shutdown or the `shutdown` command before you turn off the NWA or remove the power. Not doing so can cause the firmware to become corrupt.

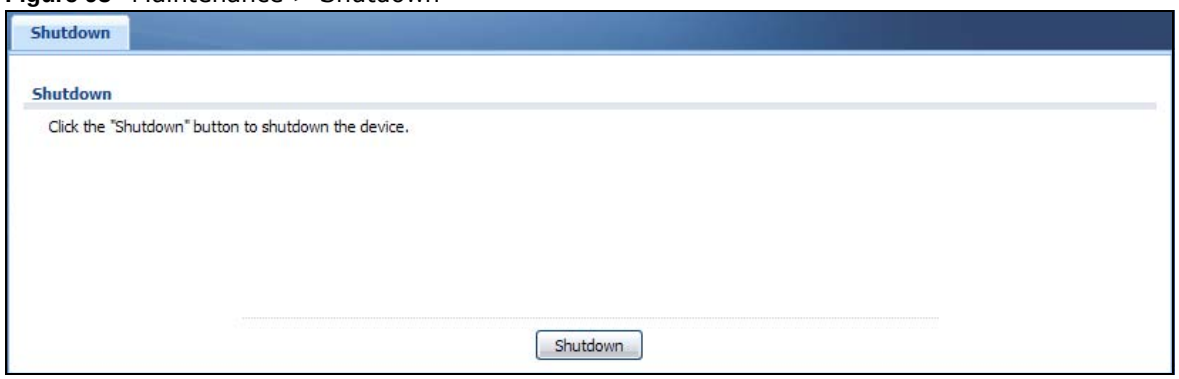
16.1.1 What You Need To Know

Shutdown writes all cached data to the local storage and stops the system processes. Shutdown is different to reset; reset returns the device to its default configuration.

16.2 Shutdown

To access this screen, click **Maintenance** > **Shutdown**.

Figure 93 Maintenance > Shutdown



Click the **Shutdown** button to shut down the NWA. Wait for the device to shut down before you manually turn off or remove the power. It does not turn off the power.

You can also use the CLI command `shutdown` to shutdown the NWA.

17

Troubleshooting

17.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LED
- NWA Access and Login
- Internet Access
- Wireless Connections
- Resetting the NWA

17.2 Power, Hardware Connections, and LED

The NWA does not turn on. The LED is not on.

1. Make sure you are using the power adaptor included with the NWA or a PoE power injector.
2. Make sure the power adaptor or PoE power injector is connected to the NWA and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or PoE power injector.
4. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
5. If none of these steps work, you may have faulty hardware and should contact your NWA vendor.

The LED does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.5 on page 17.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Disconnect and re-connect the power adaptor or PoE power injector to the NWA.

5 If the problem continues, contact the vendor.

17.3 NWA Access and Login

I forgot the IP address for the NWA.

1 The default IP address is **192.168.1.2**.

2 If you changed the IP address and have forgotten it, you have to reset the device to its factory defaults. See Section 17.6 on page 175.

3 If your NWA is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.2.
- If you changed the IP address, use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the NWA.

2 Check the hardware connections, and make sure the LED is behaving as expected. See the Quick Start Guide and Section 1.5 on page 17.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.

4 Make sure your computer is in the same subnet as the NWA. (If you know that there are routers between your computer and the NWA, skip this step.)

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address.
- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NWA.

5 Reset the device to its factory defaults, and try to access the NWA with the default IP address. See Section 17.6 on page 175.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the NWA using another service, such as Telnet. If you can access the NWA, check the remote management settings to find out why the NWA does not respond to HTTP.
- If your computer is connected wirelessly, use a computer that is connected to a **LAN**/**ETHERNET** port.

I forgot the password.

1. The default password is **1234**.
2. If this does not work, you have to reset the device to its factory defaults. See Section 17.6 on page 175.

I can see the **Login** screen, but I cannot log in to the NWA.

1. Make sure you have entered the user name and password correctly. The default password is **1234**. This fields are case-sensitive, so make sure [Caps Lock] is not on.
2. You cannot log in to the web configurator while someone is using Telnet to access the NWA. Log out of the NWA in the other session, or ask the person who is logged in to log out.
3. Disconnect and re-connect the power adaptor or PoE power injector to the NWA.
4. If this does not work, you have to reset the device to its factory defaults. See Section 17.6 on page 175.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

17.4 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LED is behaving as expected. See the Quick Start Guide and Section 17.2 on page 169.

2 Make sure the NWA is connected to a broadband modem or router with Internet access and your computer is set to obtain an dynamic IP address.

3 If you are trying to access the Internet wirelessly, make sure the wireless settings on the wireless client are the same as the settings on the NWA.

4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

5 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the NWA), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LED is behaving as expected. See the Quick Start Guide and Section 1.5 on page 17.

2 Reboot the NWA.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LED, and check Section 1.5 on page 17. If the NWA is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Check the signal strength. If the signal is weak, try moving the NWA closer to the NWA (if possible), and look around to see if there are any devices that might be interfering with the wireless network (microwaves, other wireless networks, and so on).

3 Reboot the NWA.

4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

17.5 Wireless Connections

I cannot access the NWA or ping any computer from the WLAN.

1. Make sure the wireless LAN (wireless radio) is enabled on the NWA.
2. Make sure the radio or at least one of the NWA's radios is operating in AP mode.
3. Make sure the wireless adapter (installed on your computer) is working properly.
4. Make sure the wireless adapter (installed on your computer) is IEEE 802.11 compatible and supports the same wireless standard as the NWA's active radio.
5. Make sure your computer (with a wireless adapter installed) is within the transmission range of the NWA.
6. Check that both the NWA and your computer are using the same wireless and wireless security settings.

Hackers have accessed my WEP-encrypted wireless LAN.

WEP is extremely insecure. Its encryption can be broken by an attacker, using widely-available software. It is strongly recommended that you use a more effective security mechanism. Use the strongest security mechanism that all the wireless devices in your network support. WPA2 or WPA2-PSK is recommended.

The wireless security is not following the re-authentication timer setting I specified.

If a RADIUS server authenticates wireless stations, the re-authentication timer on the RADIUS server has priority. Change the RADIUS server's configuration if you need to use a different re-authentication timer setting.

I cannot get a certificate to import into the NWA.

1. For **My Certificates**, you can import a certificate that matches a corresponding certification request that was generated by the NWA. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.
2. You must remove any spaces from the certificate's filename before you can import the certificate.
3. Any certificate that you want to import has to be in one of these file formats:
   - Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
   - PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
   - Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The NWA currently allows the importation of a PKS#7 file that contains a single certificate.

- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.
- Binary PKCS#12: This is a format for transferring public key and private key certificates.The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the NWA.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

I can only see newer logs. Older logs are missing.

When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

The commands in my configuration file or shell script are not working properly.

- In a configuration file or shell script, use "#" or "!" as the first character of a command line to have the NWA treat the line as a comment.
- Your configuration files or shell scripts can use "exit" or a command line consisting of a single "!" to have the NWA exit sub command mode.
- Include `write` commands in your scripts. Otherwise the changes will be lost when the NWA restarts. You could use multiple `write` commands in a long script.

Note: "exit" or "!'" must follow sub commands if it is to make the NWA exit sub command mode.

I cannot get the firmware uploaded using the commands.

The Web Configurator is the recommended method for uploading firmware. You only need to use the command line interface if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

Wireless clients are not being load balanced among my APs.

- Make sure that all the APs used by the wireless clients in question share the same SSID, security, and radio settings.
- Make sure that all the APs are in the same broadcast domain.
- Make sure that the wireless clients are in range of the other APs; if they are only in range of a single AP, then load balancing may not be as effective.

In the **Monitor > Wireless > AP Information > Radio List** screen, there is no load balancing indicator associated with any APs assigned to the load balancing task.

- Check to be sure that the AP profile which contains the load balancing settings is correctly assigned to the APs in question.
- The load balancing task may have been terminated because further load balancing on the APs in question is no longer required.

17.6 Resetting the NWA

If you cannot access the NWA by any method, try restarting it by turning the power off and then on again. If you still cannot access the NWA by any method or you forget the administrator password(s), you can reset the NWA to its factory-default settings. Any configuration files or shell scripts that you saved on the NWA should still be available afterwards.

Use the following procedure to reset the NWA to its factory-default settings. This overwrites the settings in the startup-config.conf file with the settings in the system-default.conf file.

Note: This procedure removes the current configuration.

1. Make sure the LED is on and not blinking.
2. Press the **RESET** button and hold it until the LED begins to blink. (This usually takes about five seconds.)
3. Release the **RESET** button, and wait for the NWA to restart.

   You should be able to access the NWA using the default settings.

17.7 Getting More Troubleshooting Help

Search for support information for your model at www.zyxel.com for more troubleshooting suggestions.

A

Importing Certificates

This appendix shows you how to import public key certificates into your web browser.

Public key certificates are used by web browsers to ensure that a secure web site is legitimate. When a certificate authority such as VeriSign, Comodo, or Network Solutions, to name a few, receives a certificate request from a website operator, they confirm that the web domain and contact information in the request match those on public record with a domain name registrar. If they match, then the certificate is issued to the website operator, who then places it on the site to be issued to all visiting web browsers to let them know that the site is legitimate.

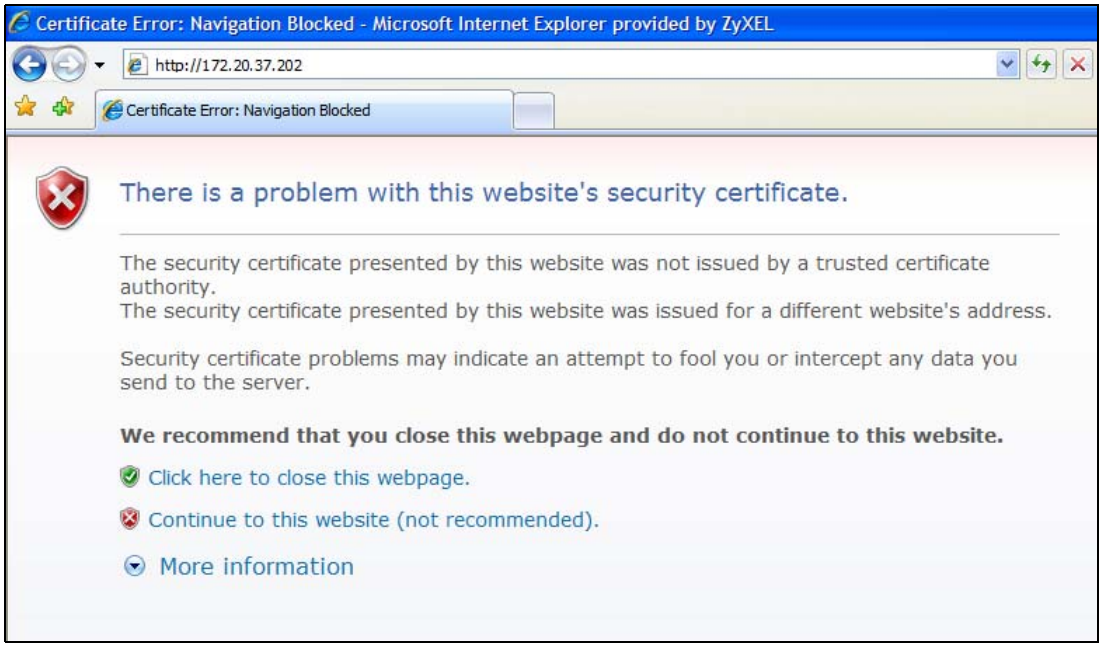
Many ZyXEL products, such as the ZyWALL, issue their own public key certificates. These can be used by web browsers on a LAN or WAN to verify that they are in fact connecting to the legitimate device and not one masquerading as it. However, because the certificates were not issued by one of the several organizations officially recognized by the most common web browsers, you will need to import the ZyXEL-created certificate into your web browser and flag that certificate as a trusted authority.

Note: You can see if you are browsing on a secure website if the URL in your web browser's address bar begins with `https://` or there is a sealed padlock icon ( ) somewhere in the main browser window (not all browsers show the padlock in the same location).

Internet Explorer

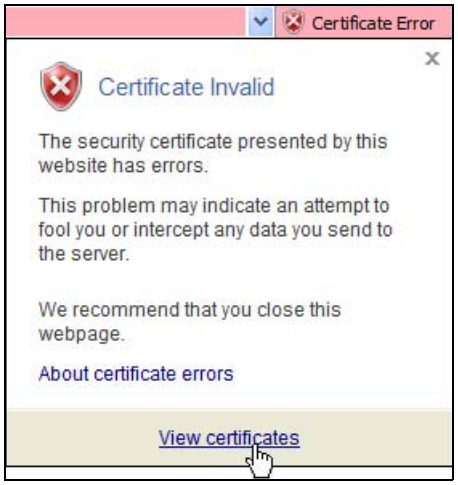
The following example uses Microsoft Internet Explorer 7 on Windows XP Professional; however, they can also apply to Internet Explorer on Windows Vista.

1 If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

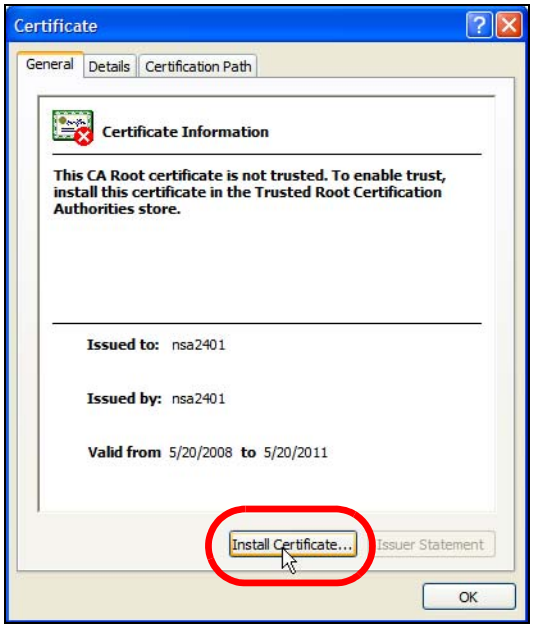

Certificate Error: Navigation Blocked - Microsoft Internet Explorer provided by ZyXEL
http://172.20.37.202
Certificate Error: Navigation Blocked
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

2 Click **Continue to this website (not recommended)**.

3 In the **Address Bar**, click **Certificate Error** > **View certificates**.


Certificate Error
Certificate Invalid
The security certificate presented by this website has errors.
This problem may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage.
About certificate errors
View certificates

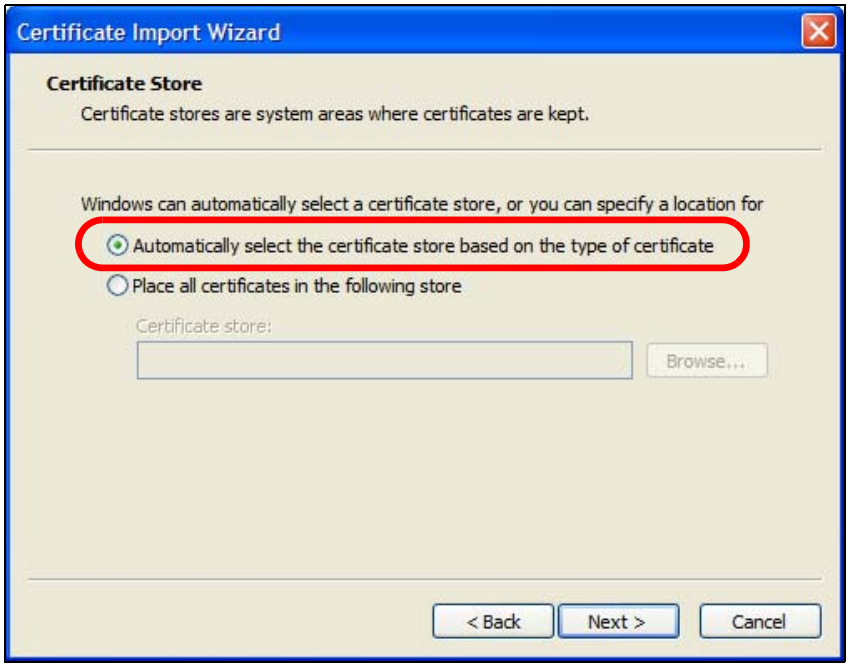
4 In the **Certificate** dialog box, click **Install Certificate**.



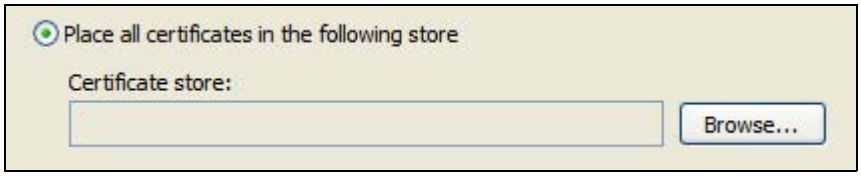
5 In the **Certificate Import Wizard**, click **Next**.

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

6 If you want Internet Explorer to **Automatically select certificate store based on the type of certificate**, click **Next** again and then go to step 9.

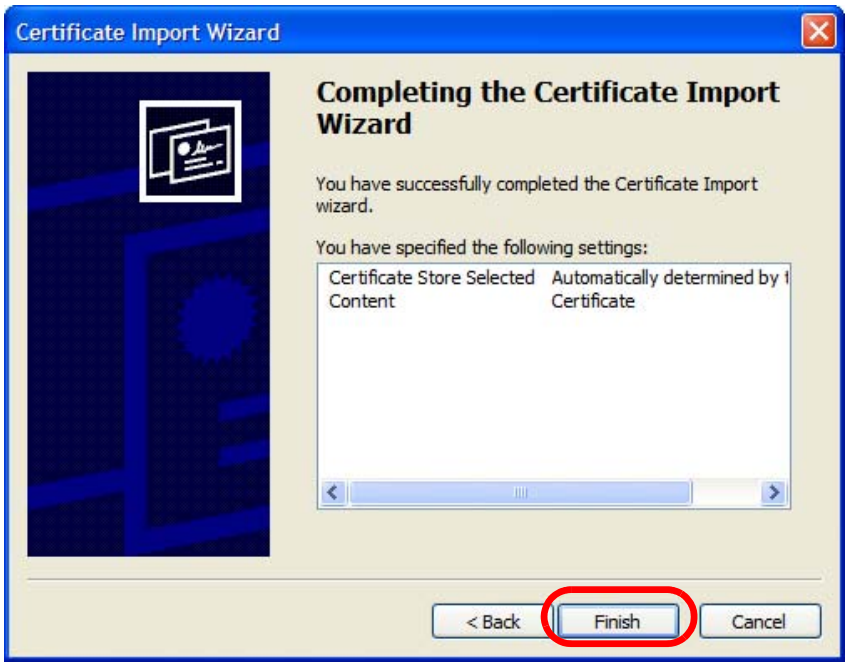

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

7 Otherwise, select **Place all certificates in the following store** and then click **Browse**.



8 In the **Select Certificate Store** dialog box, choose a location in which to save the certificate and then click **OK**.

9 In the **Completing the Certificate Import Wizard** screen, click **Finish**.

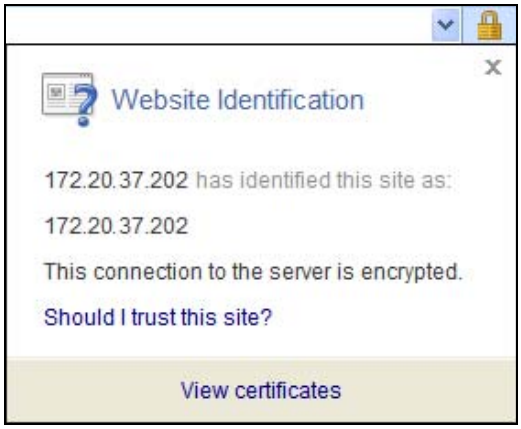


10 If you are presented with another **Security Warning**, click **Yes**.

Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
nsa2401
Windows cannot validate that the certificate is actually from "nsa2401". You should confirm its origin by contacting "nsa2401". The following number will assist you in this process:
Thumbprint (sha1): 35D1C9AC DBC0E654 FE327C71 464D154B 242E5B93
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No

11 Finally, click **OK** when presented with the successful certificate installation message.

12 The next time you start Internet Explorer and go to a ZyXEL Web Configurator page, a sealed padlock icon appears in the address bar. Click it to view the page's **Website Identification** information.



Installing a Stand-Alone Certificate File in Internet Explorer

Rather than browsing to a ZyXEL Web Configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

2 In the security warning dialog box, click **Open**.

Open File - Security Warning
Do you want to open this file?
Name: CA.cer
Publisher: Unknown Publisher
Type: Security Certificate
From: D:\Documents and Settings\13435\Desktop
Open
Cancel
Always ask before opening this file
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

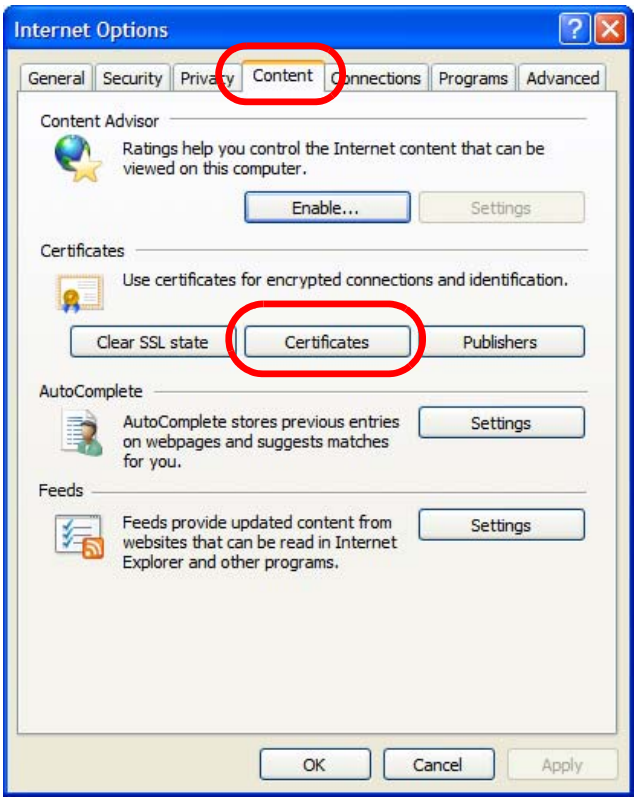
3 Refer to steps 4-12 in the Internet Explorer procedure beginning on page 177 to complete the installation process.

Removing a Certificate in Internet Explorer

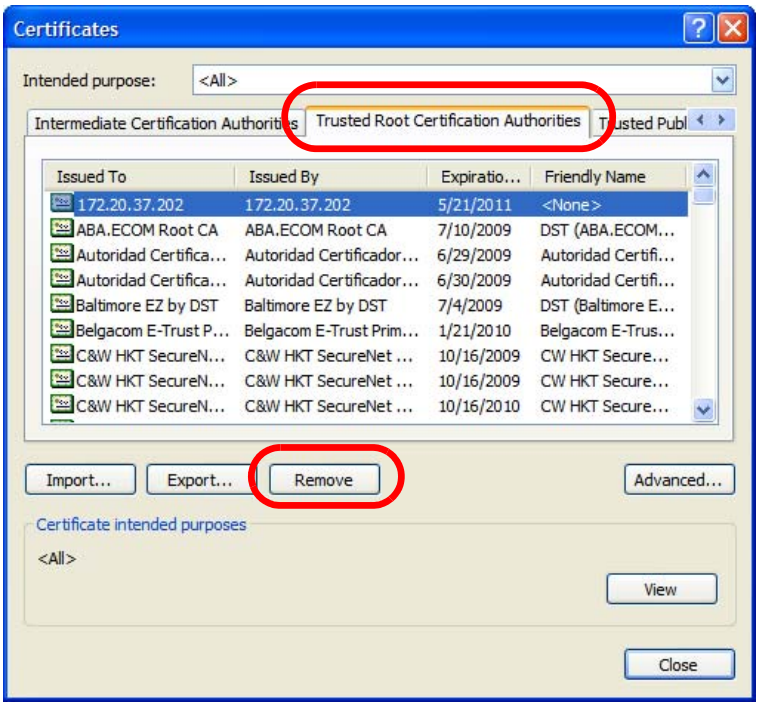
This section shows you how to remove a public key certificate in Internet Explorer 7 on Windows XP.

1 Open **Internet Explorer** and click **Tools > Internet Options**.

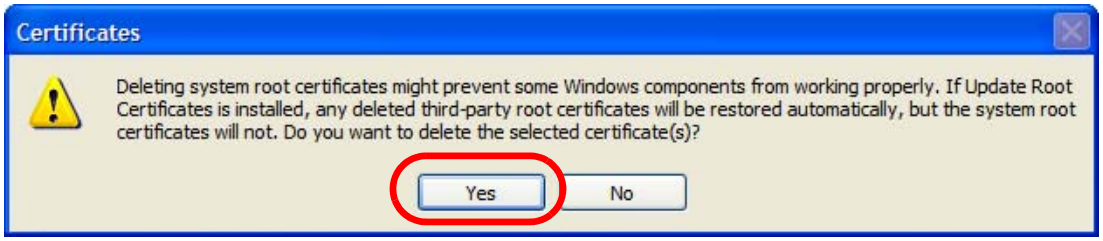
2 In the **Internet Options** dialog box, click **Content** > **Certificates**.



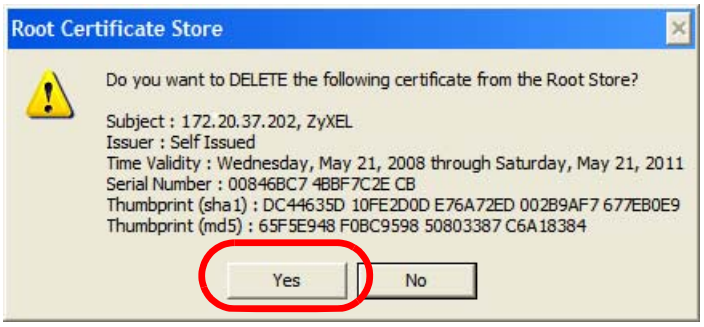
3 In the **Certificates** dialog box, click the **Trusted Root Certificates Authorities** tab, select the certificate that you want to delete, and then click **Remove**.



4 In the **Certificates** confirmation, click **Yes**.


Certificates
Deleting system root certificates might prevent some Windows components from working properly. If Update Root Certificates is installed, any deleted third-party root certificates will be restored automatically, but the system root certificates will not. Do you want to delete the selected certificate(s)?
Yes
No

5 In the **Root Certificate Store** dialog box, click **Yes**.


Root Certificate Store
Do you want to DELETE the following certificate from the Root Store?
Subject : 172.20.37.202, ZyXEL
Issuer : Self Issued
Time Validity : Wednesday, May 21, 2008 through Saturday, May 21, 2011
Serial Number : 00846BC7 4BBF7C2E CB
Thumbprint (sha1) : DC44635D 10FE2D0D E76A72ED 002B9AF7 677EB0E9
Thumbprint (md5) : 65F5E948 F0BC9598 50803387 C6A18384
Yes
No

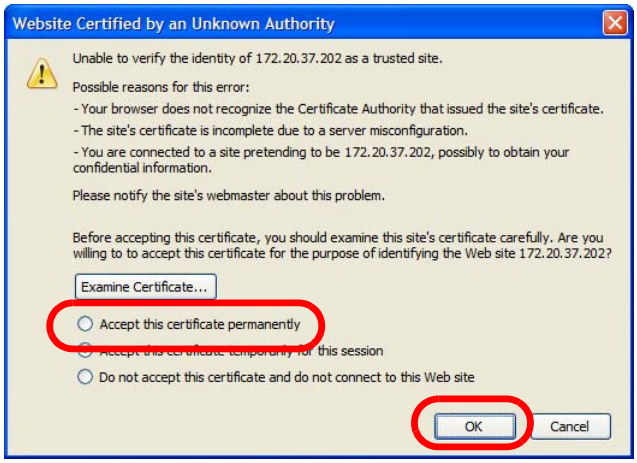
6 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

Firefox

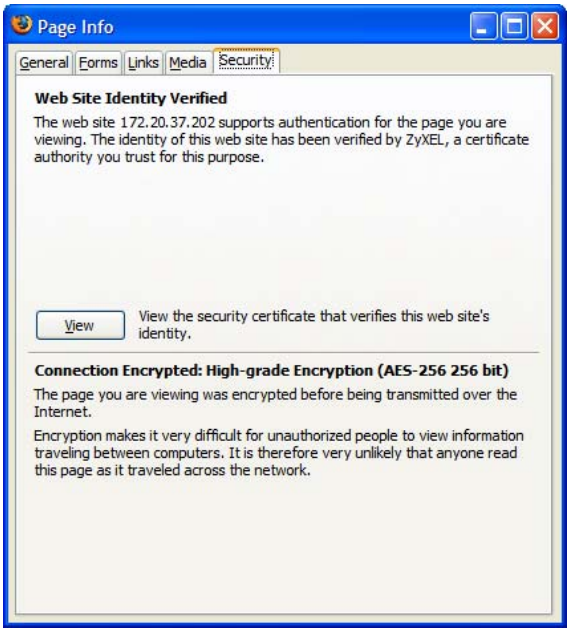
The following example uses Mozilla Firefox 2 on Windows XP Professional; however, the screens can also apply to Firefox 2 on all platforms.

1 If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

2 Select **Accept this certificate permanently** and click **OK.**


Website Certified by an Unknown Authority
Unable to verify the identity of 172.20.37.202 as a trusted site.
Possible reasons for this error:
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be 172.20.37.202, possibly to obtain your confidential information.
Please notify the site's webmaster about this problem.
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site 172.20.37.202?
Examine Certificate...
Accept this certificate permanently
Do not accept this certificate and do not connect to this Web site
OK
Cancel

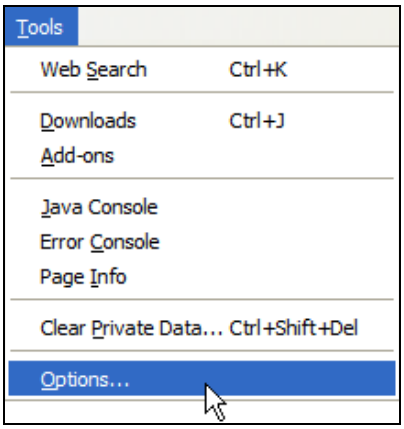
3 The certificate is stored and you can now connect securely to the Web Configurator. A sealed padlock appears in the address bar, which you can click to open the **Page Info > Security** window to view the web page's security information.


Page Info
General
Forms
Links
Media
Security
Web Site Identity Verified
The web site 172.20.37.202 supports authentication for the page you are viewing. The identity of this web site has been verified by ZyXEL, a certificate authority you trust for this purpose.
View
View the security certificate that verifies this web site's identity.
Connection Encrypted: High-grade Encryption (AES-256 256 bit)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

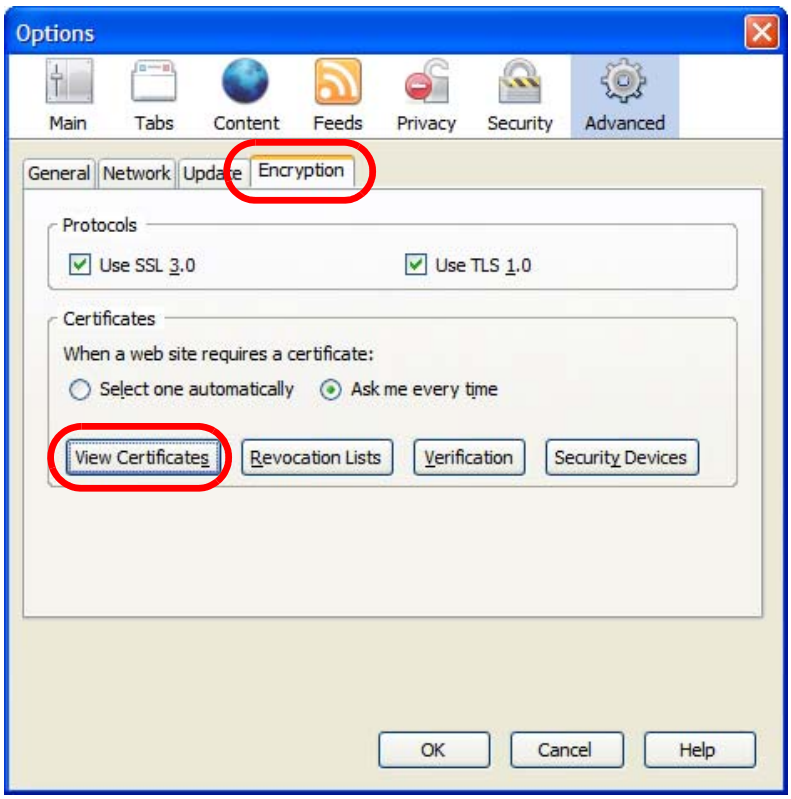
Installing a Stand-Alone Certificate File in Firefox

Rather than browsing to a ZyXEL Web Configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

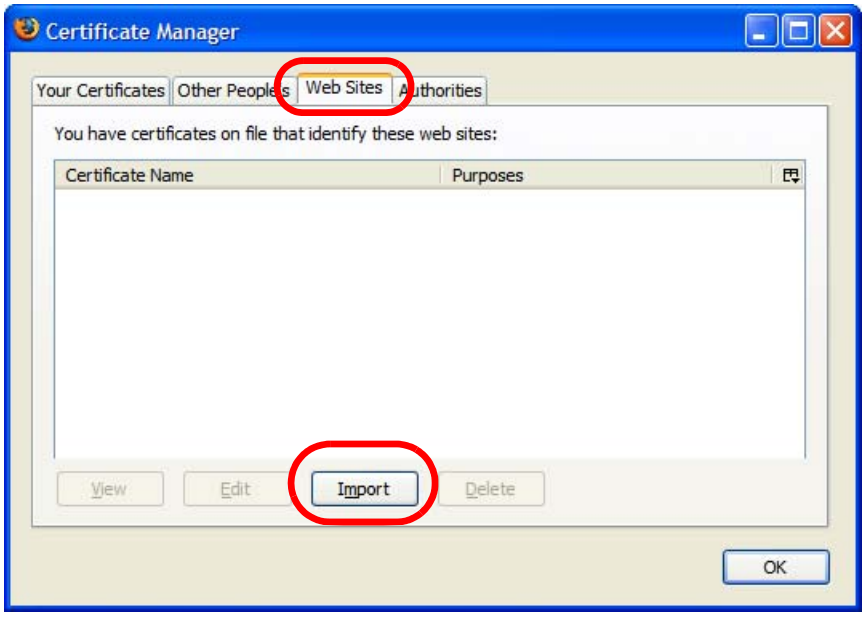
1 Open **Firefox** and click **Tools > Options**.



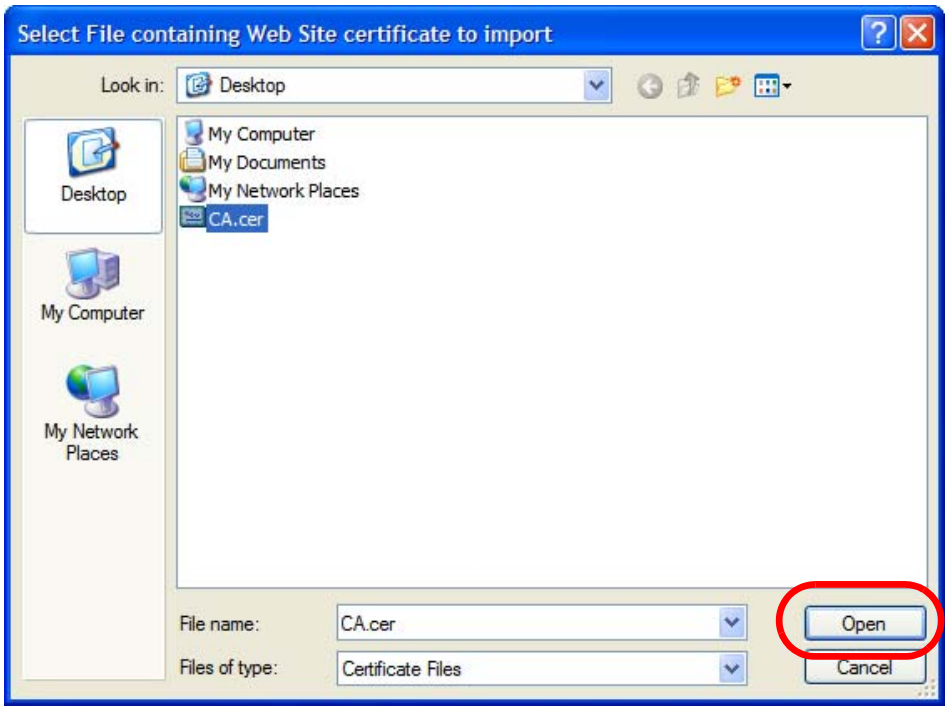
2 In the **Options** dialog box, click **Advanced** > **Encryption** > **View Certificates**.



3 In the **Certificate Manager** dialog box, click **Web Sites** > **Import**.



4 Use the **Select File** dialog box to locate the certificate and then click **Open**.

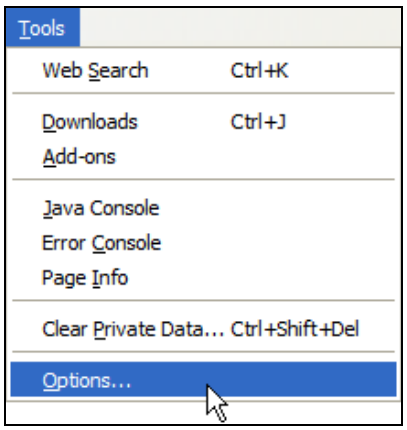


5 The next time you visit the web site, click the padlock in the address bar to open the **Page Info** > **Security** window to see the web page's security information.

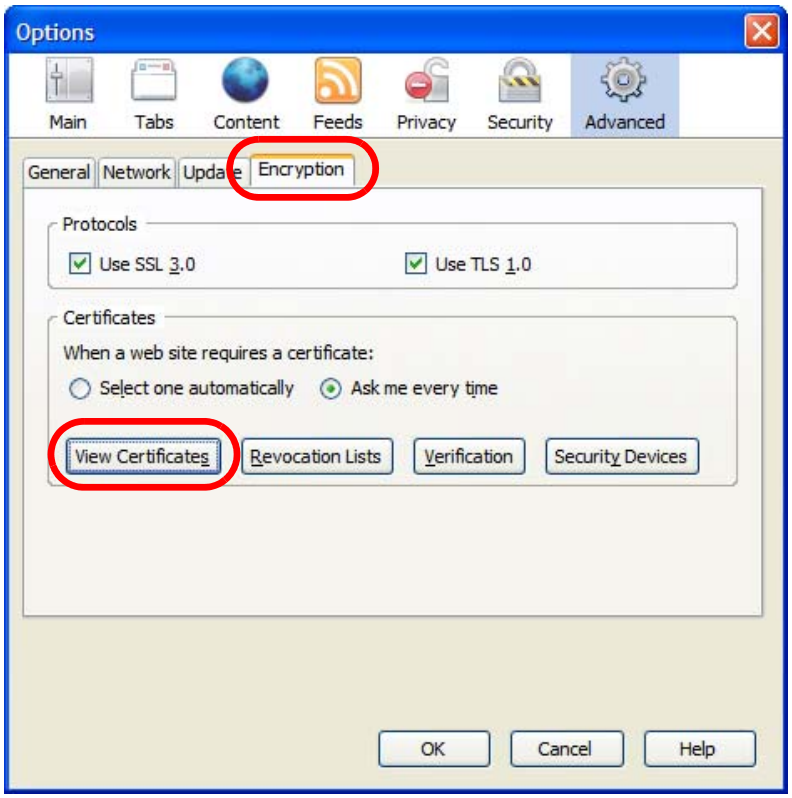
Removing a Certificate in Firefox

This section shows you how to remove a public key certificate in Firefox 2.

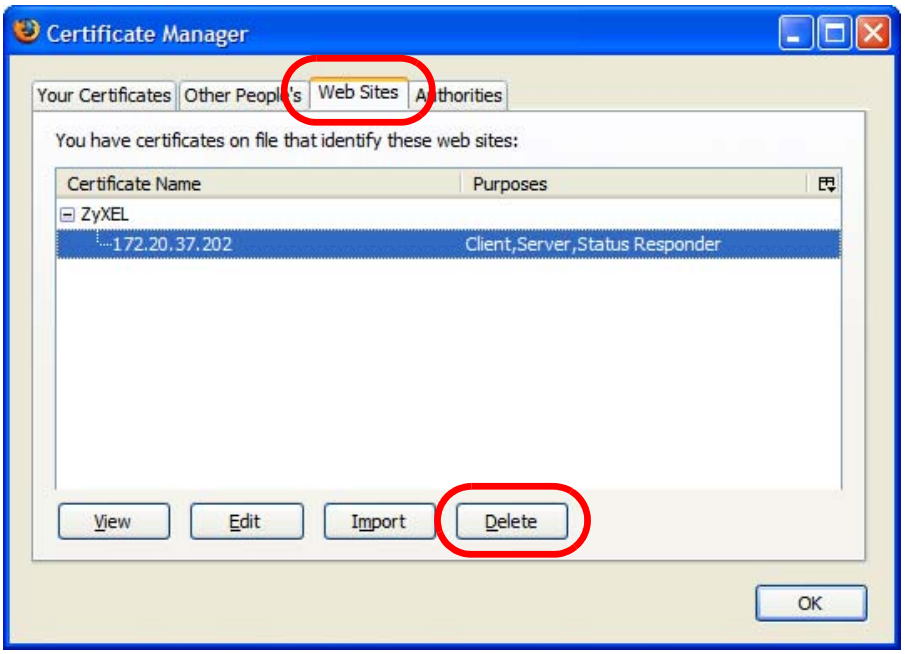
1 Open **Firefox** and click **Tools** > **Options**.



2 In the **Options** dialog box, click **Advanced** > **Encryption** > **View Certificates**.



3 In the **Certificate Manager** dialog box, select the **Web Sites** tab, select the certificate that you want to remove, and then click **Delete**.



4 In the **Delete Web Site Certificates** dialog box, click **OK**.

Delete Web Site Certificates
Are you sure you want to delete these web site certificates?
172.20.37.202
If you delete a web site certificate, you will be asked to accept it again the next time you visit the web site.
OK
Cancel

5 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

B

Legal Information

Copyright

Copyright © 2013 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimers

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Your use of the NWA is subject to the terms and conditions of any related service providers.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment.
- IEEE 802.11b, 802.11g or 802.11n (20MHz) operation of this product in the U.S.A. is firmware-limited to channels 1 through 11. IEEE 802.11n (40MHz) operation of this product in the U.S.A. is firmware-limited to channels 3 through 9.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

1) this device may not cause interference and

2) this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 3dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

IC Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.

注意 ！

依據　低功率電波輻射性電機管理辦法
第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。
在 5.25-5.35 (GHz) 頻帶內操作之無線資訊傳輸設備，限於室內使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

ErP (Energy-related Products) Declaration of Conformity

All ZyXEL products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive).

This product has been outside the scope of Energy efficiency limitation requirement in the light of the terms of Regulation (EC) No 1275/2008, Annex II:

2. Four years after this Regulation has come into force:

(c) Availability of off mode and/or standby mode

Equipment shall, except where this is inappropriate for the intended use, provide off mode and/or standby mode, and/or another condition which does not exceed the applicable power consumption requirements for off mode and/or standby mode when the equipment is connected to the mains power source.

(d) Power management

-another condition which does not exceed the applicable power consumption requirements for off mode and/or standby mode when the equipment is connected to the mains power source. The power anagement function shall be activated before delivery.

4. Information to be provided by manufacturers:

(c) the characteristics of equipment relevant for assessing conformity with the requirements set out in point 1(c), or the requirements set out in points 2(c) and/or 2(d), as applicable, including the time taken to automatically reach standby, or off mode, or another condition which does not exceed the applicable power consumption requirements for off mode and/or standby mode.

In particular, if applicable, the technical justification shall be provided that the requirements set out in point 1(c), or the requirements set out in points 2(c) and/or 2(d), are inappropriate for the intended use of equipment.

EU Directive & Regulation:

ErP Directive: Directive 2009/125/EC

Standby & off mode: Regulation (EC) No 1275/2008,

Guidance accompanying Commission Regulation (EC) No 1275/2008,

source: http://ec.europa.eu/energy/efficiency/ecodesign/eco_design_en.htm

Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Regulatory Information

European Union

The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)

Compliance Information for 2.4GHz and 5GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 1999/5/EC (R&TTE Directive)

[Czech]	ZyXEL tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
[Danish]	Undertegnede ZyXEL erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
[German]	Hiermit erklärt ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
[Estonian]	Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, ZyXEL declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
[Spanish]	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
[Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ZyXEL ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕC.
[French]	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
[Italian]	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
[Latvian]	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
[Lithuanian]	Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
[Dutch]	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
[Maltese]	Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
[Hungarian]	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EK irányelv egyéb előírásainak.
[Polish]	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
[Portuguese]	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
[Slovenian]	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
[Slovak]	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
[Finnish]	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[Swedish]	Härmed intygar ZyXEL att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
[Bulgarian]	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/ЕС.
[Icelandic]	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.
[Norwegian]	Erklærer herved ZyXEL at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 1999/5/EF.
[Romanian]	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 1999/5/EC.

CE

National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2, 4- and 5-GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries inwhich additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. ZyXEL recommends that you check with the local authorities for the latest status of their national regulations for both the 2,4- and 5-GHz wireless LANs.

The following countries have restrictions and/or requirements in addition to those given in the table labeled "*Overview of Regulatory Requirements for Wireless LANs*":.

Overview of Regulatory Requirements for Wireless LANs			
Frequency Band (MHz)	Max Power Level (EIRP)[1] (mW)	Indoor ONLY	Indoor and Outdoor
2400-2483.5	100		V
5150-5350	200	V	
5470-5725	1000		V

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.

Denmark

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.

Latvia

The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.

2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used(specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Malta	MT
Belgium	BE	Netherlands	NL
Cyprus	CY	Poland	PL
Czech Republic	CR	Portugal	PT
Denmark	DK	Slovakia	SK
Estonia	EE	Slovenia	SI
Finland	FI	Spain	ES
France	FR	Sweden	SE
Germany	DE	United Kingdom	GB
Greece	GR	Iceland	IS
Hungary	HU	Liechtenstein	LI
Ireland	IE	Norway	NO
Italy	IT	Switzerland	CH
Latvia	LV	Bulgaria	BG
Lithuania	LT	Romania	RO
Luxembourg	LU	Turkey	TR

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- The PoE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.
- This product is for indoor use only (utilisation intérieure exclusivement).
- FOR COUNTRY CODE SELECTION USAGE (WLAN DEVICES)
  Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all Wi-Fi product marketed in US must fixed to US operation channels only.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

RoHS

ENGLISH	DEUTSCH	ESPAÑOL	FRANÇAIS
Green Product Declaration RoHS Directive 2011/65/EU WEEE Directive 2002/96/EC (WEEE: Waste Electrical and Electronic Equipment) 2003/108/EC;2008/34/EC Declaration Signature: Name/Title: Thomas Wei / Quality Management Department/ Senior Director. Date (yyyy/mm/dd): 2012/07/09	**Grünes Produkt Erklärung** RoHS Richtlinie 2011/65/EU ElektroG Richtlinie 2002/96/EG (ElektroG: Über Elektro- und Elektronik-Altgeräte) 2003/108/EG;2008/34/EG Unterschrift des Erklärenden: Name/Title: Thomas Wei / Quality Management Department/ Senior Director. Date (yyyy/mm/dd): 2012/07/09	**Declaración de Producto Ecológico** Directiva RoHS 2011/65/UE Directiva RAEE 2002/96/CE (RAEE : Residuos de Aparatos Eléctricos y Electrónicos) 2003/108/CE;2008/34/CE Firma de declaración: Nombre/Título: Thomas Wei / Quality Management Department/ Senior Director. Fecha (aaaa/mm/dd): 2012/07/09	**Déclaration de Produit Vert** Directive RoHS 2011/65/UE Directive DEEE 2002/96/CE (DEEE : déchets d'équipements électriques et électroniques) 2003/108/CE;2008/34/CE Signature de la déclaration : Nom/Titre : Thomas Wei / Quality Management Department/ Senior Director. Date (aaaa/mm/jj) : 2012/07/09
ITALIANO	**NEDERLANDS**	**SVENSKA**	
Prodotto dichiarazione di verde Direttiva RoHS 2011/65/UE Direttiva RAEE 2002/96/CE (RAEE: Rifiuti di Apparecchiature Elettriche ed Elettroniche) 2003/108/CE;2008/34/CE Firma dichiarazione: Nome/titolo: Thomas Wei / Quality Management Department/ Senior Director. Data (aaaa/mm/gg): 2012/07/09	**Productmilieuverklaring** RoHS Richtlijn 2011/65/EU AEEA-Richtlijn 2002/96/EG (AEEA: Afgedankte Elektrische en Elektronische apparatuur) 2003/108/EG;2008/34/EG Verklaringshandtekening: Naam/titel: Thomas Wei / Quality Management Department/ Senior Director. Datum(jjjj/mm/dd): 2012/07/09	**Miljödeklaration** RoHS Direktiv 2011/65/EU WEEE Direktiv 2002/96/EG (WEEE: om avfall som utgörs av eller innehåller elektriska eller elektroniska produkter) 2003/108/EG;2008/34/EG Deklaration undertecknad av: Namn/Titel: Thomas Wei / Quality Management Department/ Senior Director. Datum (åååå/mm/dd): 2012/07/09	

Index

Symbols

A

access 19
access privileges 14
access users 65
  see also users 65
admin users 65
  multiple logins 70
  see also users 65
alerts 141, 144, 145, 147, 148, 149
applications
  MBSSID 14

B

backing up configuration files 153
Basic Service Set
  see BSS
boot module 158
BSS 14

C

CA
  and certificates 96
CA (Certificate Authority), see certificates
CEF (Common Event Format) 142, 147
Certificate Authority (CA)
  see certificates
Certificate Management Protocol (CMP) 102
Certificate Revocation List (CRL) 96
  vs OCSP 111
certificates 95
  advantages of 96
  and CA 96
  and FTP 133
  and HTTPS 118
  and SSH 130
  and WWW 120
  certification path 96, 104, 109
  expired 96
  factory-default 96
  file formats 96
  fingerprints 105, 110
  importing 99
  not used for encryption 96
  revoked 96
  self-signed 96, 101
  serial number 104, 109
  storage space 98, 107
  thumbprint algorithms 97
  thumbprints 97
  used for authentication 96
  verifying fingerprints 97
certification requests 101, 102
certifications 191
  notices 192
  viewing 192
channel 15
CLI 16, 24
  button 24
  messages 24
  popup window 24
cold start 18
commands 16
  sent by Web Configurator 24
Common Event Format (CEF) 142, 147
comparison table 13
configuration 13
  information 163
configuration files 151
  at restart 153
  backing up 153
  downloading 154
  downloading with FTP 133

editing 151
how applied 152
lastgood.conf 153, 156
managing 152
startup-config.conf 156
startup-config-bad.conf 153
syntax 151
system-default.conf 156
uploading 156
uploading with FTP 133
use without restart 151
cookies 19
copyright 191
CPU usage 34, 36
current date/time 34, 114
daylight savings 115
setting manually 117
time server 117

D

date 114
daylight savings 115
DCS 54
DHCP 114
and domain name 114
diagnostics 163
Digital Signature Algorithm public-key algorithm, see DSA
disclaimer 191
documentation
related 2
domain name 114
DSA 101
dual radios 14
dual-radio application 15
dynamic channel selection 54

E

e-mail
daily statistics report 140
encryption
RSA 104
ESSID 173
Extended Service Set IDentification 73

F

FCC interference statement 191
file extensions
configuration files 151
shell scripts 151
file manager 151
Firefox 19
firmware
and restart 157
boot module, see boot module
current version 34, 158
getting updated 157
uploading 157, 158
uploading with FTP 133
flash usage 34
FTP 16, 133
and certificates 133
with Transport Layer Security (TLS) 133

G

Guide
Quick Start 2

H

HTTP
over SSL, see HTTPS
redirect to HTTPS 120
vs HTTPS 119
HTTPS 118
and certificates 118
authenticating clients 119
avoiding warning messages 122
example 121
vs HTTP 119
with Internet Explorer 121
with Netscape Navigator 121

HyperText Transfer Protocol over Secure Socket Layer, see HTTPS

I

IEEE 802.1x 74
installation 13
interface
  status 35
interfaces
  as DHCP servers 114
interference 15
Internet Explorer 19
Internet telephony 14
IP Address 51
  gateway IP address 51

J

Java
  permissions 19
JavaScripts 19

K

key pairs 95

L

lastgood.conf 153, 156
layer-2 isolation 88
  example 88
  MAC 88
LEDs 17
  Blinking 17
  Flashing 17
  Off 17
load balancing 54
log messages
  categories 145, 147, 148, 149
  debugging 47
  regular 47
  types of 47
logout
  Web Configurator 22
logs
  e-mail profiles 141
  e-mailing log messages 49, 144
  formats 142
  log consolidation 145
  settings 141
  syslog servers 141
  system 141
  types of 141

M

MAC address
  range 34
maintenance 13
management 13
Management Information Base (MIB) 134, 135
management mode 15
managing the device
  good habits 16
  using FTP. See FTP.
MBSSID 14
memory usage 34, 37
message bar 27
messages
  CLI 24
  warning 27
mode
  managed mode 15
  standalone 15
mode changge 15
model name 34
My Certificates, see also certificates 98

N

Netscape Navigator 19
network access control 13
Network Time Protocol (NTP) 116

O

objects
certificates 95
users, account
user 65
Online Certificate Status Protocol (OCSP) 111
vs CRL 111
other documentation 2
overview 13

P

packet
statistics 42
physical ports
packet statistics 42
pop-up windows 19
power off 18
power on 18
product registration 192
Public-Key Infrastructure (PKI) 96
public-private key pairs 95

Q

Quick Start Guide 2

R

radio 15
reboot 18, 165
vs reset 165
registration
product 192
related documentation 2
remote management
FTP, see FTP
Telnet 132
WWW, see WWW
reports
daily 140
daily e-mail 140
reset 175
vs reboot 165
vs shutdown 167
RESET button 18, 175
restart 165
RF interference 15
RFC
2510 (Certificate Management Protocol or CMP) 102
Rivest, Shamir and Adleman public-key algorithm (RSA) 101
RSA 101, 104, 110

S

SCEP (Simple Certificate Enrollment Protocol) 102
screen resolution 19
Secure Socket Layer, see SSL
serial number 34
service control
and users 118
limitations 118
timeouts 118
Service Set 73
Service Set Identifier
see SSID
shell scripts 151
downloading 160
editing 159
how applied 152
managing 160
syntax 151
uploading 161
shutdown 18, 167
vs reset 167
Simple Certificate Enrollment Protocol (SCEP) 102
Simple Network Management Protocol, see SNMP
SNMP 133, 134
agents 134
Get 134
GetNext 134
Manager 134
managers 134

MIB 134, 135
network components 134
Set 134
Trap 134
traps 135
versions 133
SSH 128
and certificates 130
client requirements 130
encryption methods 130
for secure Telnet 131
how connection is established 129
versions 130
with Linux 131
with Microsoft Windows 131
SSID 14
SSID profile
pre-configured 14
SSID profiles 14
SSL 118
starting the device 17
startup-config.conf 156
if errors 153
missing at restart 153
present at restart 153
startup-config-bad.conf 153
station 54
statistics
daily e-mail report 140
status 33
status bar 27
warning message popup 27
stopping the device 17
subnet mask 51
supported browsers 19
syslog 142, 147
syslog servers, see also logs
system log, see logs
system name 34, 114
system uptime 34
system-default.conf 156

T

Telnet 132
with SSH 131
time 114
time servers (default) 116
trademarks 191
Transport Layer Security (TLS) 133
troubleshooting 163
Trusted Certificates, see also certificates 106

U

upgrading
firmware 157
uploading
configuration files 156
firmware 157
shell scripts 159
usage
CPU 34, 36
flash 34
memory 34, 37
onboard flash 34
use 13
user authentication 65
user name
rules 66
user objects 65
users 65
access, see also access users
admin (type) 65
admin, see also admin users
and service control 118
currently logged in 34
default lease time 69, 71
default reauthentication time 70, 71
lease time 68
limited-admin (type) 65
lockout 70
reauthentication time 68
types of 65
user (type) 65
user names 66

V

Vantage Report (VRPT) 142, 147
VoIP 14
VRPT (Vantage Report) 142, 147

W

warm start 18
warning message popup 27
warranty 192
  note 192
Web Configurator 16, 19
  access 19
  requirements 19
  supported browsers 19
web configurator 13
WEP (Wired Equivalent Privacy) 74
Wi-Fi Protected Access 74
wireless channel 173
wireless client 54
wireless LAN 173
Wireless network
  overview 53
wireless network
  example 53
wireless profile 73
  layer-2 isolation 73
  MAC filtering 73
  radio 73
  security 73
  SSID 73
wireless security 14, 173
wireless station 54
WLAN interface 15
WPA 74
WPA2 74
WWW 120
  and certificates 120
  see also HTTP, HTTPS 120